

Einleitung

Der Netscape Run Length Bug ist ein Bug, der bei allen Netscape-Browsern der Generation 4.x auftritt. Das besonders kritische an diesem Bug ist, daß er auf den Plattformen Apple Macintosh und Microsoft Windows relativ häufig, auf Unix-Plattformen seltener auftritt. Er schlägt auf jeder Plattform an anderen Stellen zu und teilweise sogar bei jedem Aufruf an einer anderen Stelle.

Lange Zeit jedoch sah es so aus, als träte der Bug nur auf Apple Macintosh und Windows-Plattformen auf und dort auch jeweils an festen Stellen. Inzwischen ist jedoch zumindest von Windows-Plattformen und ebenso auch von Linux bekannt, daß dort die Einschlagstelle von Aufruf zu Aufruf wechseln kann, ohne daß sich am Dokument etwas geändert hat.

In der deutschen [JavaScript-News-Gruppe](#) besitzt dieser Bug einen eigenen Thread. Nachfolgende Zitate sind meine Postings und einige andere Postings in diesen Thread über diesen Bug und einigen anderen Threads, in denen sich ebenfalls dieser Bug als Ursache des Problems des Fragestellers herauskristallisierte.

Zitate aus der News-Gruppe

06 Aug 1999 20:20:41

<37AB2778.DE5A3026@gmx.de>

Ein alter Bekannter auf Apple Macintosh ist offenbar immer noch nicht beseitigt. Stand: Netscape Communicator 4.5

Den Bug hatte ich erstmal mit Netscape 4.03 bemerkt. Er hat also bereits eine längere Tradition und wurde schon mehrfach in dieser NG sowohl von mir als auch von anderen Autoren erwähnt. Die Tatsache, daß dieser Bug nun eine schon so lange Tradition besitzt, läßt sofort die Hoffnung aufkommen, daß uns dieser Bug auch noch in ferner Zukunft erhalten bleibt (so wie das A20-Gate jetzt auch beim Athlon, auch wenn wohl keiner weiß, wozu das gut sein soll). Ich gebe daher dem Unhold nun einen Namen und nenne ihn "Netscape Run Length Bug" auf daß sich jeder mit ihm vertraut mache und anfreunde, denn dieser Bug wird uns sicher noch des öfteren so manchen Stirnrunzler entlocken.

Ich habe auf dem Mac keinen neueren Browser als den 4.5er. Auf dem Linux-Rechner mit Netscape 4.51 tritt der Bug in meinem Beispiel nicht auf! Das sollte aber nicht zu dem Schluß führen, daß dort der Bug nicht implementiert ist. Es kann durchaus sein, daß er dort auf andere Dateigeometrien anspricht als auf dem Apple Macintosh.

Die Beispiel-Datei:

<http://privat.schlund.de/Georg-Maass/Search/Master.Menu.search.de.js.php3>

In dieser Beispiel-Datei ist die Stelle, an welcher ich das Erscheinen/Nichterscheinen des Bug einstelle, mit RunLength-BUG gekennzeichnet. Es ist die 17.Zeile, wenn der Server den PHP3-Code nicht interpretiert sondern rüberschickt.

Diese Zeile ist eine JavaScript-Kommentarzeile!

~~~~~

Wie kann eine Kommentarzeile zu einem Fehler führen? Na, durch einen Browser-Bug eben. Es kommt dabei nicht auf den Inhalt an, sondern allein auf die Länge: Durch Änderung der Länge kann eingestellt werden, ob Fehler auftreten oder nicht, und es kann sogar eingestellt werden, wo die Fehler auftreten. Es genügt, diese Kommentarzeile ein paar Zeichen länger oder kürzer zu machen und schon treten Fehler auf.

Was für Fehler treten auf?

HTML-Fehler, die dafür sorgen, daß selbst Teile vom hardcoded HTML nicht interpretiert und somit auch nicht gerendert werden, so kann es z.B. vorkommen, daß lediglich der im Style-Sheet festgelegte weiße Hintergrund gezeichnet wird aber keinerlei Text erscheint. Bei anderen Längen erscheint zwar der Text, aber die Stylesheet-Definitionen werden nicht berücksichtigt. Wieder andere Längen sorgen für die unterschiedlichsten JavaScript-Fehlermeldungen. Diese lassen im Wesentlichen auf einen durcheinander gebrachten Scope zum Teil auch wieder auf Parsefehler schließen. Also ein heilloses Durcheinander im RAM.

Test:

=====

Mit Netscape 3.0 funktioniert die Suchmaschine aus bislang unbekanntem Grund nicht.

Für den Test habe ich alle benötigten Dateien in ein gezipptes tar-Archiv (.tgz) gepackt.

<http://privat.schlund.de/Georg-Maass/NRLB.tgz>

Packt das Archiv aus und behaltet die darin enthaltene Ordnerstruktur bei. Auch die Dateinamen dürfen nicht geändert werden.

Beim Auspacken entsteht ein Verzeichnis NRLB. Die Datei index.html darin enthält die Beschreibung des Bugtests sowie einen Link zur Frameset-Datei der Suchmaschine.

**26 Aug 1999 21:27:05**

[<37C59507.3D5DC37B@gmx.de>](mailto:<37C59507.3D5DC37B@gmx.de>)

Das Einfügen zusätzlicher Code-Zeilen vor der angeblich falschen Zeile hat keineswegs automatisch eine Verschiebung der Zeilennummer zu höheren Werten zur Folge, sondern es kommt durchaus vor, daß sowohl an der Zeilennummer als auch an der Fehlermeldung selbst sich nichts ändert.

Dies zeigt sehr deutlich, daß Netscape da wild drauflos fantasiert.

Am häufigsten lautet die falsche Fehlermeldung: "unterminated string literal."

Der Bug tritt meistens im ersten Skript-Block nach einem document.write auf, insbesondere dann, wenn mittels document.write ebenfalls JavaScript-Blöcke geschrieben wurden.

Wird mittels document.write ein dynamisches Laden einer JavaScript-Bibliothek angestoßen, dann hat die Länge dieser Bibliothek in der Regel keinen Einfluß auf den Bug, möglicherweise aber die Länge des Dateinamens.

Ich kommen den Details des Bugs allmählich näher.

Ist das Auftreten des Bugs erst mal lokalisiert, so ist die Länge des Fittings (Kommentarzeilen) so zu wählen, daß die Anzahl der Zeichen des Fittings genau der Anzahl der Zeichen vom Beginn des Script-Blocks, in dem der Bug auftritt, bis zu der Stelle, an welcher der Bug auftrat, entsprechen. damit wird dann erreicht, daß Netscape die den Fehler verursachenden HTML-Teile nicht mehr innerhalb des JavaScript-Blocks zu sehen glaubt, sondern vor dem <SCRIPT>-Tag, d.h. im HTML-Bereich, wo dann auch keine JavaScript-Fehler auftreten.

Ich aktualisiere heute das Bug-Demo in meiner Site. Inzwischen sind bereits 3 Dateien der Suchmaschine betroffen. Das wundert auch nicht, denn die Suchmaschine steckt voller Dynamik und genau in dem Teil von Netscape steckt ja der Bug.

**30 Aug 1999 21:33:43**

[<37CAD96.E20A5A5D@gmx.de>](mailto:37CAD96.E20A5A5D@gmx.de)

Georg Maaß wrote:

> Ich komme den Details des Bugs allmählich näher.

Wohl wissend, daß dieser Bug auch schon mit 4er Netscapes vor 4.5 auftritt, habe ich nun mal den NN4.04 drüberlaufen lassen und zu meinem Entsetzen festgestellt, daß dort der Bug an einer anderen Stelle auftritt.

Dies bedeutet, daß jede 4er Netscape-Version auf dem Mac ein individuelles Fitting als Workaround benötigt. Prost Mahlzeit!

Es ist mir unbegreiflich, wie ein so gravierender Bug sich so lange halten kann.

Ich habe immer noch nichts neueres als den 4.5er, da auch der ftp-Download-Versuch genauso scheiterte wie die vorherigen http-Downloads. In letzter Zeit ist echt der Wurm drin. Grrr. Beim Gecko hat zwar der Download geklappt, aber dafür funzt Gecko nicht richtig und zeigt weder Fehleralerts noch eine Konsole an, so daß man bei dem überhaupt nicht erfährt, warum irgendwas nicht klappt. Das kann also der selbe Bug sein wie bei den 4ern oder auch ein völlig anderes Problem.

Inzwischen hat die Suchmaschine, an der sich diese Bugs so ätzend auswirken, erheblich weiter entwickelt. Sie unterstützt jetzt endlich auf Wunsch das Abspeichern der Wissensbasen auf der lokalen Festplatte mittels LiveConnect, was bei künftigen Recherchen die vollständige OFFLINE-Arbeit ermöglicht. Auch die Optimierung der Sammelabfragen ist nun fertig.

Für morgen ist nun wieder Fitting angesagt, bis es auch auf dem Mac wieder fehlerfrei funktioniert. Stöhn! Danach geht es wieder als aktualisiertes tgz-Archiv in meine Site. Der Bug wird auch durch das derzeit dort befindliche tgz-Archiv demonstriert.

**31 Aug 1999 16:09:52**

[<37CBE230.6DF07507@gmx.de>](mailto:37CBE230.6DF07507@gmx.de)

Georg Maaß wrote:

> Ich habe immer noch nichts neueres als den 4.5er, da auch der  
> ftp-Download-Versuch genauso scheiterte wie die vorherigen http-Downloads.

Nachdem nun endlich der Download des 4.6 geklappt hat, kann ich alle Wanzenjäger trösten:

Beim NC4.6 für Macintosh tritt der NRLB exakt an der selben Stelle wie beim NC4.5 auf. Dasselbe gilt auch für den 4.06er.

Das Auftreten einer Fehlermeldung an anderer Stelle mit NN4.04 hatte eine ganz andere Ursache. Dieser stolperte über einen Tippfehler, der JS1.3 kompatibel ist. != gibt es nicht in JavaScript 1.2 bzw. 1.1. Da ich ausdrücklich immer JavaScript1.1 (für normales Zeug) bzw. JavaScript 1.2 (für privilegiertes Zeug) verlange, sollte JavaScript 1.3-Syntax in JS1.1 bzw. JS1.2-Blöcken eigentlich auch bei den Browsern

zu einer Fehlermeldung führen, die JS1.3 verstehen. Das ist zumindest bei Netscape leider nicht so.

Elender Mist! Wozu gebe ich denn ein LANGUAGE-Attribut an, wenn kein Schwein sich drum schert.

**05 Sep 1999 11:48:10**

[<37D23C59.6E35184A@gmx.de>](mailto:<37D23C59.6E35184A@gmx.de>)

ENDE DER LANGEWEILE!

Nicht nur Netscape 4.x auf Apple Macintosh ist von diesem Browser-Bug betroffen, sondern ebenso auch Netscape 4.x unter Windows!

Prost Mahlzeit!

Bislang nicht betroffen ist Netscape 4.51 unter Linux (x86).

Wolfgang Schwarz schrieb in einer PM:

> Den Bug kann ich bei mir (NN4.5/win95) reproduzieren: Wenn ich in  
> suchen.de.php3 zwei // wegmache, kommt eine unsinnige Fehlermeldung  
> ueber Zeile 160 blabla.

Bislang nachgewiesen wurde der Bug unter folgenden Browsern:

NN 4.04, Mac  
NC 4.06, Mac  
NC 4.5, Mac  
NN 4.5, Win95  
NC 4.6, Mac

Damit dürfte dieser Bug und die als Workarround dienenden Fittings (Kommentarzeilen bestimmter Länge) auch für diejenigen Leute wieder an Interesse gewinnen, bei denen der Mac keine Priorität genießt.

Es ist also kein Bug Mac, sondern ein Netscape-Bug!

**08 Sep 1999 20:53:50**

[<37D6B0B5.BFBE176B@gmx.de>](mailto:<37D6B0B5.BFBE176B@gmx.de>)

Wolfgang Schwarz wrote:

> Soweit ich dem Bug bisher begegnet bin, besteht er einfach darin, dass  
> NN im Quelltext einen ungewünschten Zeilenumbruch einfüegt - mit view  
> source kann man ihn sogar sehen.

Was view source anzeigt, sieht unter Linux oft völlig anders aus als auf dem Mac. Wahrscheinlich sieht es unter Windows nochmals anders aus.

> Der Zeilenumbruch wird an eine ganz  
> bestimmte Stelle gesetzt, so dass man ihn durch Hinzufuegen oder  
> Wegnehmen von Zeichen vor dieser Stelle hin- und herschieben kann.  
> Wenn man ihn an eine Stelle schiebt, wo sowieso ein Zeilenumbruch  
> steht, stoert er nicht. Dazu muessen dann auch keine tausend  
> Fuellzeichen eingefuegt werden.  
> Ich glaube mal, dass das so war.

Auf dem Mac sieht man den Fehler im Source nicht! Auf dem Mac ist das auch nicht nur ein ominöser Zeilenumbruch, was da hin und hergeschoben wird, sondern es sind ganze Teile aus den document.write / document.write -Ausgaben, die sich da mit dem eigentlichen Document-Inhalt vermischen. Daß dies so ist, sehe ich auf dem Mac nicht im Source, sondern in der JavaScript-Konsole, wo ja bei der Fehlermeldung oft auch ein Code-Zitat dabei ist.

Beim Unterminated String sieht das dann in der Regel so aus, als habest Du recht mit dem Zeilenumbruch. Manchmal aber endet die scheinbar Fehlerhafte Zeile aber nicht abrupt, sondern geht plötzlich mit Codefragmenten weiter, die vorher mit document.write oder document.write ausgegeben wurden. Wenn es sich bei diesen Codefragmenten um HTML handelt, dann führt dies garantiert zu JavaScript-Fehlermeldungen. Handelt es sich aber bei diesen Codefragmenten um JavaScript und zerrupft einem dieses keine Zeile, dann ist sogar denkbar, daß es fehlerfrei ausgeführt wird, was dann aber dazuführt, daß letztlich alles außer Kontrolle gerät, weil etwas völlig anderes ausgeführt wird, als an der entsprechende Stelle im Source der Seite steht.

Dieser Bug ist ein absoluter Hammer-Bug. Man könnte den Bug mißbrauchen, um beim Lesen des Scriptes eine völlig andere Funktionalität vorzutäuschen, als tatsächlich besteht. Das dürfte jedoch in ein ätzendes Gefummel ausarten. Aber theoretisch ist das denkbar.

> > Ist das Auftreten des Bugs erst mal lokalisiert, so ist die Länge des  
> > Fittings (Kommentarzeilen) so zu wählen, daß die Anzahl der Zeichen des  
> [...]  
> Versteh ich nicht. Kannst du das nochmal erklären?

Der Script-Block, in welchem Netscape einen Fehler gefunden zu haben glaubt, fängt ja irgendwo mit <SCRIPT> an. In der Konsole markiert Netscape in der Regel auch noch das Zeichen, bei welchem er den Fehler entdeckt zu haben glaubt. Jetzt zählst Du die Anzahl der Zeichen vom < des <SCRIPT>-Tags bis zu dem von Netscape als Fehlerstelle gekennzeichneten Zeichen. Das können schnell mal 1000 oder 2000 Zeichen sein. Dies ist die Länge des Fittings, das Du in einem Script-Block davor in Form eines Kommentars (kann ruhig mehrzeilig sein, wobei dann eventuelle <CR> oder <LF> mitzuzählen sind) einfügst. Hast Du es jetzt verstanden, wie ich es meinte?

**19 Sep 1999 17:19:46**

[<37CAD96.E20A5A5D@gmx.de>](mailto:<37CAD96.E20A5A5D@gmx.de>)

Georg Maaß wrote:

> Wolfgang Schwarz wrote:

>

> > Soweit ich dem Bug bisher begegnet bin, besteht er einfach darin, dass  
> > NN im Quelltext einen ungewünschten Zeilenumbruch einfügt - mit view  
> > source kann man ihn sogar sehen.

>

> Was view source anzeigt, sieht unter Linux oft völlig anders aus als  
> auf dem Mac. Wahrscheinlich sieht es unter Windows nochmals  
> anders aus.

Mit view-source: als Protokollangabe vor der URL sieht man bei Netscape den Original-Source, während die Menüpunkte und Kontextmenüpunkte den Pseudosource nach Ausführung der document.write Anweisungen zeigen. Beides bringt den Fehler jedoch auf dem Mac nicht immer zum Vorschein, wenn z.B. nach document.write die kritischen Stellen gar nicht mehr im Pseudo-Source zu sehen sind. Im echten Source (view-source: in der Location-Zeile vor der URL) jedoch werden sie von Netscape auf dem Mac korrekt also ohne die Fehler dargestellt.

> > Der Zeilenumbruch wird an eine ganz  
> > bestimmte Stelle gesetzt, so dass man ihn durch Hinzufügen oder  
> > Wegnehmen von Zeichen vor dieser Stelle hin- und herschieben kann.  
> > Wenn man ihn an eine Stelle schiebt, wo sowieso ein Zeilenumbruch  
> > steht, stört er nicht. Dazu müssen dann auch keine tausend  
> > Füllzeichen eingefügt werden.

Bei manchen Codeteilen klappt das so, so daß dies eine solche Theorie nahe legt. Bei anderen Codeteilen klappt das nicht, oder gelingt mir zumindest nicht.

Wie dem auch sei. Dieses Verhalten ist jedenfalls sehr lästig.

Beispiel:

-----

Hier ein Beispiel, das sowohl einen Beleg für Wolfgangs Theorie als auch gleichzeitig eine Widerlegung dieser Theorie demonstriert. Der Bug ist komplizierter als von Wolfgang angenommen. In diesem Beispiel trifft der Bug ausschließlich HTML-Tags. Folge: Es passiert nichts; d.h. was passieren soll, geschieht nicht, und Fehlermeldungen treten auch nicht auf. Einige JavaScript-Teile werden gar nicht erst ausgeführt. HTML-Fehler führen bekanntlich nicht zu Fehlermeldungen.

In der zweituntersten Zeile wurde eigenmächtig ein Zeilenumbruch eingefügt, wie von Wolfgang geschildert.

In der sechsten Zeile (<S) jedoch ist etwas anderes passiert. Die ersten beiden Zeilen sowie die siebte Zeile (</HEAD><BODY>) entstammen jeweils einer document.write Anweisung. Das dazwischen jedoch ist eine Mischung aus Browserphantasie und Inhalten aus der JavaScript-Bibliothek, die mit der dynamisch erzeugten ersten Zeile eingebunden wird.

Netscape ergänzt also nicht einfach nur hin und wieder einen störenden

Zeilenumbruch. Das kommt auch vor. Aber dies ist nur eine Art, wie sich dieser Bug äußern kann. Hier kommt sowohl dieses Einfügen von Zeilenumbrüchen wie auch das Mischen von Code aus verschiedenen Quellen vor. Entsprechend unvorhersehbar ist, wie sich der Bug letztlich auswirkt.

```
<SCRIPT LANGUAGE="JavaScript1.1"
SCR="http://bioshp.de/Search/Bilder.Israel.de.js">
</SCRIPT>
<SCRIPT LANGUAGE="JavaScript1.1" TYPE="text/javascript">
Fname = 'http://bioshp.de/Search/Bilder.Israel.de.js';
</SCRIPT>
<S
</HEAD><BODY>
<P CLASS="zklein"><A NAME="Ende" TARGET="_top" HREF="..">[<A
TARGET="_top" HREF="..">Georg Maa(section) - Bioshop.de -
Homepage</A<]</P>
<P CLASS="klein"></P>
<HR>
<SCRIP
T LANGUAGE="JavaScript1.1" TYPE="text/javascript">
</BODY></HTML>
```

Ich vermute, daß die Verunstaltung von STYLE-Tags zu oftmals TTYLE-Tags ebenfalls ein Effekt dieses Browser-Bugs ist.

**16 Oct 1999 14:01:26**

[<38086915.1D56B0AE@gmx.de>](mailto:38086915.1D56B0AE@gmx.de)

Wolfgang Schwarz wrote:

```
> Georg Maaß wrote:
>
> > Bislang nachgewiesen wurde der Bug unter folgenden Browsern:
> [...]
> + NC4.03/win95
> + NC4.06/win95
> + NN4.08/win95
```

Ich muß leider auch NC4.7 MacOS zur Liste der Bug-Browser hinzufügen.

Die aktuelle Liste der bekannten Bug-Opfer lautet somit:

nachgewiesen:

```
-----
alle NN/NC 4.x auf Apple Macintosh bis einschließlich 4.7
NC4.03/win95
NC4.06/win95
NN4.08/win95
```

vermutet:



-----  
alle NN/NC 4.x unter Windows bis einschließlich 4.7

bislang nicht betroffen:

-----  
alle NN/NC 4.x unter Linux

Bugs:

-----  
Ich liebe Krabbeltiere. Da kann man endlich mal so richtig seinen Jagdinstinkt austoben...

MOZILLA! Wann korrigiert ihr den verdammten Bug endlich? Oder seid ihr heimliche MSIE-Benutzer? Der Bug ist doch nun wirklich alt genug, daß er von euch hätte entdeckt und beseitigt werden können.

**21 Oct 1999 22:27:33**

[<380F7732.F5DF5679@gmx.de>](mailto:380F7732.F5DF5679@gmx.de)

Ulrich Lauer wrote:

> Hallo Leute!

>

> > Bislang nachgewiesen wurde der Bug unter folgenden Browsern:

> > [...]

> > + NC4.03/win95

> > + NC4.06/win95

> > + NN4.08/win95

>

> Ich habe auf Georgs Seite gerade mit dem NC 4.7 Win NT ebenfalls zwei  
> "unterminated string literals" erzeugt (in line 359 und 412). Man darf  
wohl

> annehmen, daß der Bug auch im NC 4.7 für Win existiert?

Davon, daß auch die Win-Version von NC4.7 betroffen ist, ist auszugehen,  
aber

es wundert mich, daß Du HEUTE so einen Fehler entdeckt hast, denn ich habe  
schon seit Tagen keinen solchen Fehler mehr erhalten, da ich inzwischen den  
ganzen Code so umgestellt habe, daß nach der ersten Ausgabe eines

document.write fast kein Code mehr kommt, so daß der Bug nun zumindest in  
meinem Tests (draußen habe ich auch mit NC 4.6 WinNT) getestet, keine  
Fehlermeldungen mehr bekommen habe, weil nun der Bug erst hinter dem  
Dateiende

einschlägt, wo er keinen Schaden anrichtet. In meinen Tests hat es mit  
jeder

Wissensbasis funktioniert. Auch die Aktivierung von Stylesheets  
(?css=URLofSTYLESHEET an URL anhängen), sowie die Aktivierung einer  
Performance-Messung (?performance=1 an URL anhängen) konnte Netscape nicht  
aus

der Ruhe bringen.

03 Nov 1999 23:05:24

<[3820B1A2.97A0FBE7@gmx.de](mailto:3820B1A2.97A0FBE7@gmx.de)>

Mein Liebling hat mal wieder zugeschlagen. Diesmal hat es das Installationsprogramm für die OFFLINE-Suchmaschine in meiner Domain <http://bioshop.de/> (Georgs Experimentierkiste) erwischt. Dabei kamen weitere Kuriosa zutage.

1. Kuriosum: Es macht einen Unterschied, ob man die gedownloadete Datei per Drag&Drop auf das Browser-Fenster oder per Datei-Öffnen-Menüpunkt öffnet.

2. Kuriosum: Diesmal wurde wie in einigen anderen Fällen auch nicht einfach nur ein Linefeed an unsinniger Stelle in den Code reingehauen, sondern gleich ein rießiges Stück halbverdauert HTML-Code, was tiefere Einblicke in die Arbeitsweise von Stylesheets bei Netscape erlaubte. Diesmal war der Fehler nicht nur beim Blick in den Quelltext via Menüpunkt, sondern auch via Pseudoprotokoll view-source: zu sehen. Sonst sah man die Fehler nur bei Verwendung des Menüpunkts zum Quelltext einsehen oder gar nicht.

Zu 2.

-----  
Der von Netscape in den Quelltext reingehauene halbverdaute HTML-Code bestand aus etwa 5 Zeilen dicht gepacktem Text von je etwa 100 Zeichen Länge. Netscape renderte in diesem Einschub Teile des JavaScriptes und Teile des echten HTML-Codes. In diesem gerenderten JavaScript wurden z.B. alle Größerals und Kleinerals in entsprechende HTML-Entities umgesetzt. Im Auszug aus dem HTML-Teil wurden alle Stylöe-Sheetklassen in FONT-Tags u.ä. umgesetzt.

Mit anderen Worten: Aufgrund des Bugs kam zum Vorschein, daß Netscape 4.7 erst mal das ganze HTML4.0 im RAM in Uralt-HTML übersetzt, welches er dann zu rendern versucht. So kann man natürlich auch seine Zeit vertrödeln.

Bei dieser Umsetzung treten insbesondere dann Fehler auf, wenn im JavaScript document.write Anweisungen und insbesondere document.write Anweisungen, die Dateien dynamisch einbinden, vorkommen. Da ich sehr häufig von dieser Konstruktion Gebrauch mache, habe ich natürlich auch entsprechend oft Feindkontakt mit diesem inzwischen über 2 Jahre alten Bug.

Es ist mir diesmal nicht gelungen durch Änderungen in der Codereihenfolge, die Einschlagstelle des Bugs hinter das Dateiende zu verlegen. Mit dieser Vorgehensweise schaffte ich es lediglich, die Einschlagstelle aus dem JavaScript-Teil heraus in den HTML-Teil zu

verschieben und dabei auch den Rießen-Einschub in das bloße Auftreten eines Linefeeds zu verwandeln. Der Bug schlug dann in ein Tabellen-End-Tag ein, was zur Folge hatte, daß die Tabelle nicht mehr dargestellt wurde. Somit bleibt nur noch der Weg des Fittings, d.h. wieder mal Kommentarzeilen einfügen, deren einziger Zweck darin besteht, die Einschlagstelle des Bugs so zu verschieben, daß keine wichtigen Teile getroffen werden.

Diesmal ist kein Frameset im Spiel. Das betroffene Dokument ist ein ganz normales, flaches HTML-Dokument.

**29 Dec 1999 21:11:00**

[<386A6AD1.13B76C5B@gmx.de>](mailto:386A6AD1.13B76C5B@gmx.de)

Die unendliche Geschichte...

Er hat es schon wieder getan. D.h. der Bug ist schon eine ganze Weile wieder da, ohne daß ich dies bemerkt hätte, oder mich jemand informiert hätte, so daß auch ein Umstieg auf die ältesten noch verfügbaren Sourcen das Auftreten nicht beseitigen.

Wie äußert er sich diesmal? Beim erneuten Laden des Frame-Dokuments mit Hilfe eines JavaScript-Buttons hört Netscape schon nach etwa 10 Zeilen auf zu rendern. JavaScript wird zwar noch einige Zeilen weiter ausgeführt (nachweisbar z.B. durch alerts), aber Dokumentinhalt wird überhaupt nicht dargestellt. Die Quelltext-Ansicht sieht normal aus.

Wird das selbe Frame-Dokument über einen Link erneut geladen, dann wird zumindest der statische Dokument-Inhalt gerendert. Anschließend tritt eine JavaScript Fehlermeldung auf mit einer Zeilennummer (z.B. 394), die etwa um 100 Zeilen hinter der letzten Zeile des Dokuments (etwa 300) liegt. Dabei handelt es sich dann um einen unterminierten String Fehler.

Der Bug ist zu immer neuen Überraschungen gut.

Das Auftreten des Bugs kann durch Einschalten bzw. Abschalten von css beeinflusst werden. Im Wesentlichen läßt sich damit z.B. die Einschlagstelle beeinflussen. Das Aktivieren oder Deaktivieren von Java scheint keinen Einfluß auf den Bug zu haben.

Um den ganzen Mysterium noch die Krone auf zu setzen, scheint der Bug nur im

ONLINE-Betrieb aufzutreten. Wird die Suchmaschine dagegen mit den  
Instalalionsprogramm lokal installiert und lokal mit Protokoll file:  
gestartet,  
dann tritt das Phänomen derzeit bei mir nicht auf.

Wer sich das Mysterium angucken will, lade die Suchmaschine und betätige im  
oberen  
Frame den Button "Wissensbasis erweitern". Danach leert der mittlere Frame.  
Das  
Dokument wird zwar geladen (Quelltext ansehen, Dokument-Info), aber es wird  
nichts  
angezeigt.

<http://www.bioshop.de/Search/Suchen.de.php3>

Der Bug befindet sich mit großer Wahrscheinlichkeit in der HTML-Engine des  
Netscape. JavaScript wird NICHT blockiert. Der Browser hängt sich NICHT  
auf. Alles  
funktioniert ganz normal, bis auf den ganz unbedeutenden Schönheitsfehler,  
daß

halt absolut nichts angezeigt wird. Aber das macht ja nichts, denn Netscape  
läßt  
ja immerhin den Blick in den Quelltext zu, so daß wir uns das selber  
zusammenreimen können, was da hätte dargestellt werden sollen.

Scheiß Bug!

**16 Feb 2000 20:43:51**

[<38AAFDF5.9284A221@gmx.de>](mailto:<38AAFDF5.9284A221@gmx.de>)

Entgegen meinen bisherigen Annahmen tritt der Bug plattformspezifisch an  
unterschiedlichen Stellen auf. Meistens trifft es Netscape 4.x auf Apple  
Macintosh  
und Netscape 4.x auf Windoof-Rechnern an der der selben Stelle. Aber dies  
gilt leider  
nur meistens und keineswegs immer. Mit anderen Worten: Techniken, die den  
Bug  
herausfordern, müssen explizit sowohl auf Apple Macintosh wie auch auf  
Windows-Rechnern getestet werden. Diese Tests müssen nach jeder auch noch  
so kleinen

Änderung am Quelltext, die eine Längenänderung zur Folge hat, erneut  
durchgeführt  
werden. Schlägt der Bug an einer störenden Stelle ein, dann müssen die  
Fittings  
entsprechend angepaßt werden, damit der Bug entweder hinter dem Dateiende  
oder aber  
im Fitting selber einschlägt.

Daß der Bug plattformspezifisch auftritt merkte ich bei meinem in  
JavaScript  
geschriebenen Installationsprogramm, welches auf meinem privaten Apple  
Macintosh

fehlerfrei arbeitete, unter WinNT dagegen die Formulare nicht darstellte, weil der Bug in das FORM-Endtag des erstens Formulars einschlug. Mit einer geänderten Platzierung des Fittings lies sich dafür sorgen, daß der Bug nun auf beiden Plattformen nicht mehr elementare Teile zerschießt. In diesem Fall traf der Bug einen HTML-Tag. Genauso kann er aber auch im Script einschlagen.

Der Bug ist kein JavaScript spezifischer Bug, denn er kann auch in Dokumenten auftreten, die fast kein JavaScript beinhalten. Er tritt immer dann auf, wenn Dateien via document.write dynamisch eingebunden werden. Der Auftritt des Bugs geht nicht automatisch mit einem sichtbarwerden des Bugs einher. Schlägt der Bug hinter dem Dokument-Ende ein oder zwischen zwei Worten, dann merkt man nichts davon. Trifft er aber einen HTML-Tag oder ein JavaScript, dann fällt er natürlich auf.

Konstruktionen wie diese provozieren den Bug:

```
if(StyleSheetPath) document.write('<LINK REL="STYLESHEET"
HREF="'+StyleSheetPath+'
TYPE="text/css">');
if(SearchEnginePrefs) document.write('<SCR'+IPT LANGUAGE=\"JavaScript1.2\"
TYPE=\"text/javascript\" SRC=\"'+SearchEnginePrefs+'\"></SCR'+IPT>');
```

Also: Holzauge, sei wachsam. Wer wie ich so etwas macht, der muß besonders gründlich auf vielen Plattformen testen.

**26 Feb 2000 18:00:33**

[<38B8372D.744411C4@gmx.de>](mailto:38B8372D.744411C4@gmx.de)

Entgegen meinem bisherigen Rat, durch Fittings und Code-Umstellungen, die Einschlagstelle des Bugs hinter das Dokument-Ende zu verbannen, weil dies meinen bisherigen Beobachtungen zu Folge unkritisch erschien, muß ich mich leider korrigieren.

NRLB-Einschläge hinter dem Dokument-Ende sind keineswegs unkritisch! Sie können im Gegenteil sogar zum unter Workoholics heiß ersehnten Pausenzeichen (Blue Screen) führen.

Schlägt der NRLB in unserem Dokument ein, dann trifft er unseren Speicherbereich und bleibt somit unter unserer Kontrolle. Schlägt er dagegen hinter dem Dokument-Ende ein, dann kann er ein anderes Dokument treffen. Auf diese Weise kann z.B. der NRLB ausgelöst durch ein Frameset-Dokument in eines der

Frame-Dokumente einschlagen und dort dann seine Schadwirkung entfalten. Genauso kann er aber auch im Programmbereich des Browsers oder in einem völlig fremden Speicherbereich einschlagen, was dann unter eNTE zu Begegnungen mit Dr. Watson oder eben einem Blue Screen führt. Auf dem Apple Macintosh treten die selben Effekte mit den Mac spezifischen System-Fehlermeldungen oder gar Mausetot-Zuständen an Stelle von Dr. Watson und Blue Screen auf.

Auf Apple Macintosh und Windows schlägt der NRLB teilweise an der jeweils gleichen Stelle im Dokument, teilweise aber auch an unterschiedlichen Stellen ein. Eine Seite, die auf Apple Macintosh scheinbar bugfrei (in Wahrheit nur ohne sichtbare Symptome) funktioniert, kann unter eNTE alle Spielarten des NRLB von zerschossenen HTML-Tags, fehlfunktionierenden JavaScripten über Dr. Watson bis hin zum Blue Screen führen. Das gleiche gilt entsprechend auch umgekehrt.

Wer also NRLB provozierende Techniken einsetzt und eine fehlerfreie Funktionsweise garantieren möchte, der muß vor jeder Veröffentlichung explizit auf jeder gewünschten Zielplattform (Apple Macintosh / Windows) mit Netscape 4.x testen. Die Änderung auch nur eines einzigen Bytes kann es bereits wieder erforderlich machen, eine neue Testrunde zu starten.

**28 Feb 2000 13:42:08**

[<38BA6D20.F4055F05@j-dmedia.com>](mailto:38BA6D20.F4055F05@j-dmedia.com)

Thomas Fischer schrieb:

>  
> > Wer also NRLB provozierende Techniken einsetzt [...]  
>  
> Sind dies alle Arten von dyn. generierten Script-Blöcken,  
> egal ob intern oder extern?

Nein. Es sind bei mir immer dynamisch eingebundene .js und .css Dateien, die solche Effekte hervorrufen. Bei dynamisch erzeugten Blöcken, ohne Einbindung von Dateien in diesen dynamisch erzeugten Blöcken ist mir solch ein Effekt nicht bekannt.

Bei Netscape könnte ich JavaScript-Dateien (nicht .css) auch einfach via location = 'meinScript.js' einbinden. Diese Vorgehensweise ist aber zu keinem anderen Browser komptibel. Daher mache ich das grundsätzlich nicht so und weiß daher nicht, ob dabei der Effekt auch auftritt. Wahrscheinlich nicht, denn diese Vorgehensweise klappt immer, also auch nach onLoad, ist somit von der Technik her etwas grundsätzlich anderes, weil quasi das Dokument non destruktiv überladen wird.

Bei Stylesheet-Dateien geht dies aber nicht. Dynamisch eingebundene Stylesheet-Dateien lösen den NRLB ebenfalls aus. Bei mir binden alle Dokumente die Stylesheets dynamisch ein, weshalb bei mir jedes Dokument von diesem Bug betroffen ist.

**29 Feb 2000 13:42:08**

[<38BBA43E.32E6DC1E@j-dmedia.com>](mailto:38BBA43E.32E6DC1E@j-dmedia.com)

Wolfgang Schwarz schrieb:

```
>  
> ich hatte das auch schon mit internen Skripten, allerdings nur bei  
> komplexeren Geschichten.
```

also sowas in der Art, wobei hier keine Datei eingebunden wird (weder JavaScript noch sonst eine Datei):

```
document.write('<SCRIPT>rechenwas();document.write(\'schreib  
was...\');</SCRIPT>');
```

Wenn das so ist, dann tritt der NRLB in solchen Konstellationen zumindest sehr viel seltener auf, als wenn auf diese Weise eine Datei (JavaScript oder Stylesheet) eingebunden wird.

**16 Mar 2000 12:46:41**

[<38D0C9A1.3DE9C7E8@j-dmedia.com>](mailto:38D0C9A1.3DE9C7E8@j-dmedia.com)

Ralf Beutler schrieb:

```
>  
> <a ... onMouseOut="tausche('public', 1, 'Layer4')">  
>  
> beim Laden der Seite liefert NN folgende Fehlermeldung:  
>  
> unterminated string literal.  
>  
> tausche('pub', 1, 'La  
> .....^  
>  
> hat jemand eine Idee?
```

Hast Du irgendwo weiter vorne eine Datei (z.B. Stylesheet oder JavaScript-Bibliothek) mit `document.write('<SCRIPT SRC="blablab.js"></SCRIPT>');` oder ähnlich eingebunden?

Hast Du schon mal probiert vor die betroffene Stelle folgendes einzufügen (bitte nicht nach Sinn fragen, sondern ausprobieren):

```
<SCRIPT><!--
```

```
/*////////////////////////////////////  
////////////////////////////////////  
////////////////////////////////////  
*/ //--></SCRIPT>
```

Hilft das?

**16 Mar 2000 13:21:56**

[<8aqjp6\\$44oj5\\$1@fu-berlin.de>](mailto:8aqjp6$44oj5$1@fu-berlin.de)

Georg Maaß schrieb:

```
> Hast Du irgendwo weiter vorne eine Datei (z.B. Stylesheet oder  
> JavaScript-Bibliothek) mit document.write('<SCRIPT  
> SRC="blablab.js"></SCRIPT>'); oder ähnlich eingebunden?
```

nein, allerdings damit die Positionierungen von ie und nn übereinstimmen:

```
<script language="JavaScript">  
<!--  
document.write('<style type="text/css">');  
if(BROWSER=="NN"){  
  document.write("body {margin-top:6; margin-left:1;}");  
}  
document.write('</style>');  
//-->  
</script>
```

**16 Mar 2000 17:19:59**

[<38D109AF.51066D0E@j-dmedia.com>](mailto:38D109AF.51066D0E@j-dmedia.com)

Ralf Beutler schrieb:

```
>  
> nein, allerdings damit die Positionierungen von ie und nn übereinstimmen:  
>  
> <script language="JavaScript">  
> <!--  
> document.write('<style type="text/css">');  
> if(BROWSER=="NN"){  
>   document.write("body {margin-top:6; margin-left:1;}");  
> }  
> document.write('</style>');  
> //-->  
> </script>
```

Mir ist zwar von sowas kein solcher Effekt bekannt, aber Unkenntnis ist ja kein Beweis für Nichtexistenz; es könnte ja auch ein Bildungslücke



meinerseits sein. Ich weiß, aber, daß unter Linux, solche Dinge bei Netscape zu sehr merkwürdigen Effekten führen können, wie z.B. Scopeverlust, oder Unfähigkeit, JavaScript auszuführen und ähnlicher Kram.

> > (bitte nicht nach Sinn fragen, sondern ausprobieren):

> >

> > <SCRIPT><!--

> >

>

/\*////////////////////////////////////

/

>

////////////////////////////////////

/

> //////////////////////////////////

> > \*/ file:/--></SCRIPT>

>

> danke, ich werds probieren

Hat das denn geholfen? Wenn ja, dann haben wir eine neue Konstruktion gefunden, wie man den NRLB auslösen kann.

**16 Mar 2000 17:32:16**

[<rbeutler@mconnexion.com>](mailto:rbeutler@mconnexion.com)

Georg Maaß schrieb:

>

> Hat das denn geholfen? Wenn ja, dann haben wir eine neue Konstruktion  
> gefunden, wie man den NRLB auslösen kann.

>

> Gruß, Georg

es hat etwas gedauert, da die Sache auf PC nicht nachvollziehbar war.  
Ich musste erst an den Mac, aber

yep, es hat!!

ist aber einfach unglaublich!

Übrigens sind von diesem Phänomen auch die automatischen Scripts von Dreamweaver betroffen!

Übrigens liefert

/\*////////////////////////////////////

\*/

einen JS-Fehler.

/\*////////////////////////////////////\*/

dieses dagegen nicht.

16 Mar 2000 17:52:02

<[38D11132.859D8D11@j-dmedia.com](mailto:38D11132.859D8D11@j-dmedia.com)>

Ralf Beutler schrieb:

>

> noch eine kleine Frage:

>

> wie kommt man auf solche Lösungen?????????

Durch Zufall, indem man entdeckt, daß das Auftreten einer Fehlermeldung davon abhängt, wie lang ein Kommentar ist. Daher die Bezeichnung für den Bug: NRLB = Netscape Run Length Bug.

Mit der Kommentarlänge kann ich, je nachdem, wo der Kommentar steht entweder die Einschlagstelle des Bugs verschieben, oder aber durch geeignete Positionierung dafür sorgen, daß der Bug im Kommentara einschlägt.

Und hier die gute Nachricht:

Zu diesem Bug gibt es einen eigenen Thread in dieser NG. Was bisher geschah findest Du hier: <http://www.georg-maass.de/Hilfe/NRLB.de>. Diesen Thread werde ich ebenfalls da mit rein nehmen, denn dies ist ein Beispiel für eine mit bisher nicht bekannte Art der Auslösung des Bugs. Ich wußte aber schon von Wolfgang (Tschuldigung, falls ich mich irren sollte), daß es auch ohne dynamisches Laden einer Datei geht. Du hast nun ein Beispiel genau dafür geliefert.

Und hier die schlechte Nachricht:

Die Positionierung und Länge der Kommentare muß für Netscape 4.x auf dem Mac und für jede Netscape 4.x - Windows-Kombination speziell angepaßt werden.

17 Mar 2000 10:17:09

<[tf@team42.net](mailto:tf@team42.net)>

Georg Maaß schrieb:

>

> Die Positionierung und Länge der Kommentare muß für Netscape 4.x auf dem  
> Mac und für jede Netscape 4.x - Windows-Kombination speziell angepaßt  
> werden.

\*blauäugig\*

Sach mal Georg, gibt es eigentlich einen Zusammenhang zwischen der Position der Einschlagstelle und der Länge des dyn. geschriebenen Codes zuzüglich der dadurch ev. eingebetteten JS-File-Länge? dann wäre vielleicht auch die Plattfordmifferenz erklärbar

(unterschiedliche newline Byte-Mengen)

Wenn ja, könnte man die ganze Sache ja vielleicht automatisieren, in dem man den Dummy-Kommentar je nach Plattform dyn. generiert.

**17 Mar 2000 12:30:44**

[<38D21764.3B28C43E@j-dmedia.com>](mailto:38D21764.3B28C43E@j-dmedia.com)

Thomas Fischer schrieb:

>

> Sach mal Georg, gibt es eigentliche einen Zusammenhang  
> zwischen der Position der Einschlagstelle und der  
> Länge des dyn. geschriebenen Codes zuzüglich der  
> dadurch ev. eingebetteten JS-File-Länge?

Es gibt einen Zusammenhang zwischen dem was da dynamisch gemacht wird und der Einschlagstelle, aber dieser ist nicht linear von der Länge des dynamischen Codes abhängig. Ich kann nicht einmal sicher sagen, daß er überhaupt von dessen Länge abhängt.

In meiner Suchmaschine z.B. lösen nur die am Anfang geladenen Wissensbasen den NRLB aus, die anderen Wissensbasen nicht. Die Längen sind dabei sehr unterschiedlich (wenige hundert Bytes bis über 50 kB).

Ich bin noch nicht so weit, den NRLB gezielt auszulösen, oder dynamisch Auffangbecken für die Einschläge zu schaffen. Nicht einmal für eine einzige Plattform geschweige denn für jede betroffene Plattform.

> dann wäre vielleicht auch die Plattformdifferenz erklärbar  
> (unterschiedliche newline Byte-Mengen)

Warum ist dann ein Unterschied hinsichtlich der Einschlagstelle zwischen Win95, Win98 und WinNT?

> Wenn ja, könnte man die ganze Sache ja vielleicht automatisieren,  
> in dem man den Dummy-Kommentar je nach Plattform dyn. generiert.

Dazu müßte man mehr wissen, als ich es bislang weiß.

**17 Mar 2000 19:54:10**

[<38D27F52.1EE61DE6@j-dmedia.com>](mailto:38D27F52.1EE61DE6@j-dmedia.com)

Thomas Fischer schrieb:

>

> Obwohl am Quellcode nix geändert wird, tritt er mal auf und mal nicht???

Wenn er mit einer konkreten Rechner-Browser-Betriebssystem-Kombination auftritt, dann tritt er reproduzierbar immer an der selben Stelle auf, solange am Quelltext nichts geändert wird.

**17 Mar 2000 10:27:09**

[<8astrv\\$469rt\\$1@fu-berlin.de>](mailto:8astrv$469rt$1@fu-berlin.de)

Franz Weninger schrieb:

```
> Schau dir den Quelltext an: wahrscheinlich steht dort:  
>  
> <a ... onMouseOut="tausche('public', 1, 'La  
>  
> yer4')">  
>  
> (also ein Zeilenumbruch nach dem "a" von "Layer").
```

hi Franz,

leider war es nicht so einfach.  
Die Anweisungen stehen alle hübsch in einer Zeile.  
Es sei denn, dass beim Überspielen auf den Server irgendein Zeilenumbruch eingefügt wird.

ich habe grade nochmal den Quelltext online betrachtet:

```
<... sehr viel html in dieser Zeile...snip href="onMouseOut="tausche('pub',  
1, 'Lay  
er4')" snip... noch mehr html....>
```

Allerdings ist es sicherlich kein echter Zeilenumbruch,  
da er in meinem editor (HS) da nicht ist.  
Außerdem ist er mit dem Windowsinternen editor auch woanders.

Die Antwort vom Georg hat allerdings das Problem behoben.  
Es war sehr interessant mit der Länge von Kommentarzeichen herumzuspielen  
und so das Layout der Seite zu verändern.  
Je nach Länge des kommentars ignorierte NN die css-Anweisungen einzelner  
Ebenen,  
womit dann auch deren Positionierung zu vergessen war.

**17 Mar 2000 12:35:08**

[<38D2186C.E639135@j-dmedia.com>](mailto:38D2186C.E639135@j-dmedia.com)

Ralf Beutler schrieb:

```
>
```

> Die Anweisungen stehen alle hübsch in einer Zeile.  
> Es sei denn, dass beim Überspielen auf den Server irgendein Zeilenumbruch  
> eingefügt wird.

Der Zeilenumbruch oder mehr Schrottkode wird von Netscape dynamisch dort eingefügt und löst damit dann je nach Einschlagstzelle JavaScript-Fehler oder HTML-Fehler aus. Dies ist das typische Kennzeichen für den NRLB.

Schlägt das Teil in einem Kommetar ein, dann stört dieser Mist nicht. Genau darin besteht der Trick mit dem Kommentar.

Bisher habe ich immer JavaScript-Kommentare genommen, aber mit HTML-Kommentaren müßte das genauso gehen.

**19 Mar 2000 19:25:36**

[<38D51B9E.12A1D0D8@gmx.de>](mailto:38D51B9E.12A1D0D8@gmx.de)

Ist der NRLB möglicherweise älter als bislang vermutet?

Folgendes Fehlerprotokoll ist heute bei mir eingegangen:

---

User-Agent: Mozilla/3.01Gold (Macintosh; I; 68K)  
User-Adr: 212.144.64.83 64-83.M.dial.o-tel-o.net

Fehler: JavaScript (caught by javacgi.js)  
Zeile: 25  
Datei:  
http://www.georg-  
maass.de/Suite/Dokumentation/library.de.html?css=index.mm&eMail=&JavaScript  
=active

Datum/Zeit: Sun 19.March.2000 11:09:51  
missing ) after condition

---

Um die kritisierte Stelle herum befindet sich im Original-Quelltext folgender Code:

```
<script language="JavaScript" TYPE="text/javascript" CHARSET="ISO-8859-1"><!--  
if(parent.Content && parent.Content.getHeader)  
document.write(parent.Content.getHeader(self));  
if(parent.Content && parent.Content.getBackground)  
document.write(parent.Content.getBackground(self)); else  
if(parent.setBackground) parent.setBackground(self); else  
document.write('<\/HEAD><BODY>');  
if(parent.Content && parent.Content.getBody)  
document.write(parent.Content.getBody(self));  
/--><\/SCRIPT>
```

Die mittlere Zeile ist Zeile 25. Die JavaScript-Bibliothek wird vorher statisch eingebunden. Zeile 25 in der JavaScript-Bibliothek enthält den Bug-Catcher. Hätte dieser den fehlerverursacht, dann wäre das Protokoll nicht versandt worden.

Ich habe darauf hin die Seite sowohl mit NN4.7 als auch mit meinem NN3.01 Mozilla/3.01 [de]-C-MACOS8 (Macintosh; I; PPC) getestet. Es tritt bei beiden keine Fehlermeldung auf. Ich habe aber auch einen Blick in den Quelltext geworfen mit Netscape 3.01 als Quelltext-Anzeige-Programm. Folgendes zeigt mein NN3.01 auf dem Mac an:

```
-----
<SCRIPT LANGUAGE="JavaScript1.1" TYPE="text/javascript"
SRC="../../../JavaScriptEngine/javacg<link REL="STYLESHEET"
HREF="http://www.bioshop.de/css/index.mm.css" TYPE="text/css">
</head><body>

<p CLASS="zklein"><a NAME="Anfang" TARGET="_top" HREF="../../../"><img
SRC="../../../images/logo.gif" WIDTH="100" HEIGHT="25" BORDER="0" ALT="Georg
Maa&szlig; - Bioshop.de"></a><br>[<a TARGET="_top" HREF="../../../">Georg
Maa(section) - Bioshop.de - Homepage</a>]</p>
<p CLASS="klein"><a HREF="../menu.de.html">Georgs
Experimentierkiste</a></p> <h1>JavaScript-Bibliotheken</h1>
-----
```

Werfe ich dagegen die Stylesheet-Angabe aus der URL raus (css= statt css=index.mm), dann zeigt er mir folgendes an:

```
-----
<SCRIPT LANGUAGE="JavaScript1.1" TYPE="text/javascript"
SRC="../../../JavaScriptEngine/javacgi.js">

</SCRIPT>
<script language="JavaScript1.1" TYPE="text/javascript" CHARSET="ISO-8859-
1">

<!C-
if(self.initCgi)
{
    initCgi();
    self.onload = cgiInherit;
}
if(self.cgiStyleSheetPath) document.write('<LINK REL="STYLESHEET"
HREF="'+self.cgiStyleSheetPath+' " TYPE="text/css">');
</head><body>

<p CLASS="zklein"><a NAME="Anfang" TARGET="_top" HREF="../../../"><img
SRC="../../../images/logo.gif" WIDTH="100" HEIGHT="25" BORDER="0" ALT="Georg
Maa&szlig; - Bioshop.de"></a><br>[<a TARGET="_top" HREF="../../../">Georg
Maa(section) - Bioshop.de - Homepage</a>]</p>
<p CLASS="klein"><a HREF="../menu.de.html">Georgs
Experimentierkiste</a></p>
<h1>JavaScript-Bibliotheken</h1>
-----
```

Diese Art, den WYSIWYG-Source zu verhunzen, erinnert doch sehr an NRLB. Ich sehe also auf dem Server nach, ob der Esel vielleicht das Stylesheet geladen hat, obwohl er damit doch gar nichts anfangen kann.

Im Access Log File finde ich erwartungsgemäß Folgendes:

```
192.168.0.1      -      -      [19/Mar/2000:17:34:17 +0100]      "GET
/Suite/Dokumentation/library.de.html?css=index.mm&Mail=&JavaScript=active
HTTP/1.0"      200      9874      "-"      "Mozilla/4.7 (Macintosh; I; PPC) "
```

```
192.168.0.1      -      -      [19/Mar/2000:17:34:18 +0100]      "GET
/css/index.mm.css HTTP/1.0"      200      3731      "-"      "Mozilla/4.7
(Macintosh; I; PPC) "
```

```
192.168.0.1      -      -      [19/Mar/2000:17:35:34 +0100]      "GET
/Suite/Dokumentation/library.de.html?css=index.mm&Mail=&JavaScript=active
HTTP/1.0"      200      9874      "-"      "Mozilla/3.01 [de]-C-MACOS8
(Macintosh; I; PPC) "
```

```
192.168.0.1      -      -      [19/Mar/2000:17:35:34 +0100]      "GET
/images/logo.gif HTTP/1.0"      304      -      "http://www.georg-
maass.de/Suite/Dokumentation/library.de.html?css=index.mm&Mail=&JavaScript
=active"      "Mozilla/3.01 [de]-C-MACOS8 (Macintosh; I; PPC) "
```

```
192.168.0.1      -      -      [19/Mar/2000:17:35:35 +0100]      "GET
/JavaScriptEngine/javacgi.js HTTP/1.0"      304      -      "-"
"Mozilla/3.01 [de]-C-MACOS8 (Macintosh; I; PPC) "
```

Der Status 200 bedeutet, daß die Datei erfolgreich übertragen wurde, 304 bedeutet, daß der Server diese Anfrage aus seinem eigenen Cache bedienen konnte. NN3.01 hat die HTML-Datei, das Logo und die JavaScript-Bibliothek geladen. Für das Stylesheet hat er sich nicht interessiert. NN4.7 hat sich nicht für das Logo interessiert, weil er es im eigenen Cache gefunden hatte und meine Webkonfiguration auf "Cache niemals überprüfen" eingestellt ist. Die Browser haben also netzwerkmäßig das gemacht, was sie sollten. NN3.01 hat das Stylesheet nicht geladen, was völlig korrekt ist.

Das Acceslog-File vom März habe ich noch nit, so daß ich noch nicht nachprüfen kann, ob etwa die 68K-Version des NN3.01 fälschlicher Weise das Stylesheet geladen hat. Ich glaube es aber nicht. Wenn also bei der 68K-Version trotzdem ein NRLB ausgelöst worden ist, dann kann er nicht durch das Stylesheet ausgelöst worden sein, sondern allein vom document.write, welches von der Angabe eines Stylesheets mittels des cgi-Parameters css=STYLESHEET getriggert wird.

Ich hoffe, daß der Besucher, der diesen Bug-Report ausgelöst hat, unter uns weilt und mit dem selben Browser (und geleertem Cache) die Seite erneut aufruft, diesmal aber ohne Stylesheet-Angabe, also am besten alle cgi-Parameter weglassen.  
<http://www.georg-maass.de/Suite/Dokumentation/library.de.html> Wenn diesmal dann kein Bug-Report ausgelöst wird, dann haben wir wieder einige Informationen über den NRLB hinzugewonnen.

Dann wissen wir definitiv, daß er schon im 3er Netscape vorhanden ist und unter unglücklichen Umständen von JEDEM document.write ausgelöst werden kann. Tritt der Fehler wieder auf, dann wissen wir lediglich,

daß es das document.write, das von der Stylesheet-Angabe getriggert wird, nicht war. Es sind aber noch mehr document.writes da. Der Übergang vom Head zum Body wird ebenfalls via document.write realisiert, da ich so im Kontext des zugehörigen Framesets dynamisch die Hintergründe, Text- und Linkfarben festlegen kann.

Die kritisierte Zeile (Zeile 25) macht genau dies.

In meinen eigenen Tests mit den PowerPC-Versionen der Netscape-Browser tritt kein solches Problem auf. Auch mit NN2.01 tritt kein Problem auf. Wenn ich mit diesem Fossil den Quelltext ansehe, dann wird der Quelltext korrekt dargestellt, obwohl auch dieser zumindest das document.write ausführt, welches das Ende des Head und den Anfang des Body einleitet. An dem anderen document.write kommt er nie vorbei, da sich dieses in einem JavaScript1.1-Block befindet.

Sollte der NRLB also mit NN3.0 das Licht der Welt erblickt haben?

Mozilla M14; Mozilla/5.0 (Macintosh; N; PPC; en-US) Mozilla/m13 findet auch keinen Anlaß zu irgendwelchen Beanstandungen und zeigt den Quelltext ebenfalls korrekt an. Warum er sich im userAgent allerdings als m13 ausgibt, weiß ich auch nicht, denn es ist definitiv ein M14, wie die about-Seite bestätigt.

Und so siehts im NN4.7 mit Stylesheet aus:

```
-----
<SCRIPT LANGUAGE="JavaScript1.1" TYPE="text/javascript"
SRC="../../JavaScriptEngine/javacgi.js">

</SCRIPT>
<LINK REL="STYLESHEET" HREF="http://www.bioshop.de/css/index.mm.css"
TYPE="text/css">
</HEAD><BODY>

<P CLASS="zklein"><A NAME="Anfang" TARGET="_top" HREF="../../"><IMG
SRC="../../images/logo.gif" WIDTH="100" HEIGHT="25" BORDER="0" ALT="Georg
Maa&szlig; - Bioshop.de"></A><BR>[<A TARGET="_top" HREF="../../">Georg Maaß
- Bioshop.de - Homepage</A>]</P>
<P CLASS="klein"><A HREF="../../menu.de.html">Georgs
Experimentierkiste</A></P>
<H1>JavaScript-Bibliotheken</H1>
-----
```

und so ohne Stylesheet:

```
-----
<SCRIPT LANGUAGE="JavaScript1.1" TYPE="text/javascript"
SRC="../../JavaScriptEngine/javacgi.js">

</SCRIPT>
<script language="JavaScript1.1" TYPE="text/javascript" CHARSET="ISO-8859-
1">

<!--
```



```

if(self.initCgi)
{
    initCgi();
    self.onload = cgiInherit;
}
if(self.cgiStyleSheetPath) document.write('<LINK REL="STYLESHEET"
HREF="'+self.cgiStyleSheetPath+' " TYPE="text/css">');
// -->

</script>
</HEAD><BODY>

<P CLASS="zklein"><A NAME="Anfang" TARGET="_top" HREF="../../"><IMG
SRC="../../images/logo.gif" WIDTH="100" HEIGHT="25" BORDER="0" ALT="Georg
Maa&szlig; - Bioshop.de"></A><BR>[<A TARGET="_top" HREF="../../">Georg
Maa(section) - Bioshop.de - Homepage</A>]</P>
<P CLASS="klein"><A HREF="../menu.de.html">Georgs
Experimentierkiste</A></P>
<H1>JavaScript-Bibliotheken</H1>
-----

```

Das hat also sehr viel Ähnlichkeit mit dem, was der 3er anzeigt.

Sicher ist nur eines: Die Seite hat keine JavaScript Fehler. Alle anders lautenden Beteuerungen der Browser sind Browser-Bugs, NRLB oder andere Bugs.

**01 Apr 2000 13:12:59**

[38E5D9BB.4C1DAB25@kcl.ac.uk](mailto:38E5D9BB.4C1DAB25@kcl.ac.uk)

ich habe den NRLB mal soweit isoliert, dass man ihn schoen untersuchen kann. Man braucht keine eingebundenen Dateien, es reicht, wenn per document.write css-definitionen geschrieben werden. Hier meine Datei:

```

<html>
<head>
<title></title>
<SCRIPT LANGUAGE="JavaScript" TYPE="text/javascript">
<!--
document.write('\
<style type="text/css">\n\
.pop {width:100}\
</style>\
');
// -->
</script>
<SCRIPT LANGUAGE="JavaScript" TYPE="text/javascript">
<!--
str="bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla";
str="bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla";

```

Diese Zeile wiederholt sich insgesamt 55 mal.

```
//-->
</SCRIPT>
</head>
<body>
</body>
</html>
```

```
JavaScript Error: line 66:
unterminated string literal.
str="bla bla bla bla bla bla
....^
```

Erste Ergebnisse der Obduktion:

- Es muss etwas in den Styles stehen, nur `<style></style>` zu schreiben reicht nicht. Was da drin steht ist aber egal.

- Es muessen zwei Script-Blocke da sein. Wenn man das

```
// -->
</script>
<SCRIPT LANGUAGE="JavaScript" TYPE="text/javascript">
<!--
```

rausnimmt, verschwindet der Fehler. Das ist seltsam, weil der Bug bekanntlich auch ausserhalb von Script-Blocken im HTML-Bereich auftaucht.

- Ob die Scripte im Head oder Body stehen spielt keine Rolle.

Einen Zusammenhang zwischen dem Style-Geschreibsel und der Einschlagstelle habe ich noch nicht gefunden. Vielleicht mag ja jemand mal mittesten.

Interessant ist auch, wieso bei dansteinman der Bug in der Regel nicht zum Vorschein kommt, obwohl der dauernd style-Tags schreibt (mit seinen css und writeCSS-Funktionen).

Soviel erstmal.

Gruss,  
Wolfgang.

**2 Apr 2000 22:36:47**

[<8c8i16\\$skp\\$1@news04.btx.dtag.de>](mailto:8c8i16$skp$1@news04.btx.dtag.de)

Wolfgang Schwarz <wolfgang.schwarz@kcl.ac.uk> schrieb:  
>

```
> [...] Vielleicht mag ja jemand mal mittesten.
```

```
Habe mal kurz rumgespielt (leider zu wenig Zeit)  
Wenn die Styles so geschrieben werden
```

```
document.write('<style type="text/css">\n.pop {width:100}</style>');
```

```
tritt der NRLB nicht auf
```

```
salute
```

```
Thomas Fischer (derdreiviertelvorzwölfte)
```

*03 Apr 2000 22:35:05*

```
dreimal seh Herr F.,
```

```
Thomas Fischer wrote:
```

```
> Wenn die Styles so geschrieben werden
```

```
>
```

```
> document.write('<style type="text/css">\n.pop {width:100}</style>');
```

```
>
```

```
> tritt der NRLB nicht auf
```

```
mhm. So auch nicht:
```

```
document.write('\n\n<style type="text/css">\n\n.pop {width:100}\n\n</style>')
```

```
Aber so schon:
```

```
document.write('<style type="text/css">.pop {width:100}</style>\n')  
                                         ^^
```

```
Und so auch:
```

```
document.write('<style type="text/css">.pop {width:100}</style>')  
                ^^
```

```
So ebenfalls:
```

```
document.write('<style type="text/css">.pop {width:100}</style>\r')  
                                         ^^
```

```
Und so:
```

```
document.write('<style type="text/css">.pop {width:100}')  
document.write('</style>\n')
```

```
Und selbst so:
```

```
document.write('<style type="text/css">.pop {width:100}</style> bla\n')
```

```
Aber so nicht:
```

```
document.write('<style type="text/css">.pop {width:100}</style>')
document.write('\n')
```

Daher erster Verdacht und Vorschlag fuer einen workaround:

Der NRLB wird ausgeloeset, wenn ein abschliessender style-tag mit nachfolgendem Zeilenumbruch in `_einer_ document.write`-Anweisung geschrieben wird.

Workaround (das waere wirklich lustig): Einfach kein write und am Ende kein `\n` benutzen beim dynamischen style-Schreiben.

Jetzt muesste man natuerlich noch Beispiele untersuchen, wo der Bug auftritt. Georg, hast du noch ein paar? Ralf hatte neulich auch einen. Wie ists bei euch?

Und mal bei dan steinman kucken, bei dem wie gesagt kein Bug auftaucht... aha, sieht gut aus:

```
function writeCSS(str, showAlert) {
    str = css('START')+str+css('END')
    document.write(str)
}
...
mit
function css(id, left, top, width, height, color, vis, z, other) {
    if (id=="START") return '<STYLE TYPE="text/css">\n'
    else if (id=="END") return '</STYLE>'
}
...
```

Wolfgang.

**04 Apr 2000 11:48:11**

Ich muß einfach mal die bislang bekannten Varianten durchforsten, bei denen das mit einem einfachen `document.write` auftrittt, ob da keines dabei ist, das nicht ohne newline endet. Wenn dieser einfache Workaround allgemein funktioniert, dann wäre zumindest mal das Problem für solche Fälle ohne externe Datei gelöst.

Dann wäre als nächstes zu prüfen, ob denn das Entfernen des abschließenden newlines in den externen Dateien eine Auswirkung auf den NRLB hat. Sollte deren Entfernung ebenfalls eine Trigger-Wirkung haben, dann wäre das ein echter Durchbruch im Kampf gegen diesen Bug.

Gruß, Georg

**04 Apr 2000 11:54:12**

Ich habe gerade in meinem NRLB-Archiv  
<http://www.georg-maass.de/Hilfe/NRLB.de.html> in meiner Domain  
nachgeguckt:

Ralf Beutler schrieb:

```
>  
> nein, allerdings damit die Positionierungen von ie und nn  
übereinstimmen:
```

```
>  
> <script language="JavaScript">  
> <!--  
> document.write('<style type="text/css">');  
> if(BROWSER=="NN"){  
>   document.write("body {margin-top:6; margin-left:1;}");  
> }  
> document.write('</style>');  
> //-->  
> </script>
```

Dieses Beispiel endet auch mit einem newline. Das wäre ja echt ein  
Hammer, wenn sich das Auftreten des Bugs durch entfernen des newline  
abstellen ließe.

Gruß, Georg

**04 Apr 2000 21:11:06**

Auf meinem privaten Mac mit NC4.7 schlägt der NRLB exakt an der selben  
Stelle wie von Wolfgang angegeben ein. Es verhält sich alles genau so wie  
von Wolfgang beschrieben. Hier haben wir es also mal nicht mit  
Plattformunterschieden zu tun.

Auch das Verschwinden des Bugs nach Entfernen des newlines ist auf meinem  
privaten Mac genau so wie von Wolfgang geschildert.

Gruß, Georg

**07 Apr 2000 23:36:44**

[<38EE54E2.3EBFA21E@gmx.de>](mailto:38EE54E2.3EBFA21E@gmx.de)

Georg Maaß wrote:

```
> Auch das Verschwinden des Bugs nach Entfernen des newlines ist auf meinem  
> privaten Mac genau so wie von Wolfgang geschildert.
```

Ich habe inzwischen aus allen Style-Sheets, die ich ja bekanntlich  
dynamisch  
einbinde, die newlines am Dateiende entfernt. Trotzdem ist soeben eine NRLB

eingeschlagen. Nachdem ich aber aus dem document.write, mit dem ich es einband ein document.write machte, verschwand der Einschlag.

Wir scheinen also wirklich sehr nahe dran zu sein.

**19 Aug 2000 23:42:57**

Georg Maaß wrote:

```
> Ich habe mal wieder einen NRLB in meiner Homepage. Diesmal im
> Frameset-Dokument. Dieses erzeugt das Frameset dynamisch, da ein
> statisches Frameset mit JavaScript-URLs inkompatibel zu JavaScript
> losen Browsern wäre. Die dynamische Erzeugung jedoch erlaubt mir die
> Verwendung eines Alternativ-Framesets in einem NOSCRIPT-Block.
>
> Die beiden Framedokumente enden beide NICHT mit einem Zeilenumbruch,
> sondern mit </HTML>. Im Frameset-Dokument, kommen in den
> document.write-Anweisungen überhaupt keine Newlines vor. Ebenso werden
> auch keine document.write verwendet.
>
> Es scheint also eine andere Variante des NRLB zu sein, die nicht mit
> der von Wolfgang identifizierten Art übereinstimmt. Die Einschlagstelle
> unterscheidet sich sowohl zwischen den verschiedenen NN4.x Versionen
> auf dem Mac als auch zwischen verschiedenen Versionen unter Window, wie
> auch unter gleichen Browser-Versionen aber unterschiedlichen
> Windows-Versionen.
>
> Im Moment bleibt mir daher nichts anderes, als mal wieder mit einem
> Fitting eine ungefährliche "Soll"-Einschlagzone zu schaffen. Elender
> Scheiß-Bug!
```

**13 Mar 2001**

NRLB in NN4.7 unter Linux

=====

```
JavaScript Error: http://bioshop.de/cgi-bin/gmL/?HTMLinfo=10, line 133:
syntax error.
```

```
if(typeof gmL!='object'&&!gmL)gmL=new<script
type="text/javascript;version=1.1">gmL.browser.jstv=1.1</script><script
type="text/javascript;version=1.2">gmL.browser.jstv=1.2</script><script
type="text/javascript;version=1.3">gmL.browser.jstv=1.3</script><s
.....^
```

```
JavaScript Error: http://bioshop.de/cgi-bin/gmL/?HTMLinfo=10, line 174:
gmL.browser.iCab has no properties.
```

JavaScript Error: http://bioshop.de/cgi-bin/gmL/?HTMLinfo=10, line 176:

gmL.browser.iCab has no properties.

Das Auftreten des NRLB unter Linux hängt von den Cache-Einstellungen ab.

Wann immer der Browser meint, irgendwas aus dem Cache holen zu können, treten obige Fehlermeldungen auf. Durch völliges Abschalten des Cache läßt sich das Problem jedoch nur mildern, nicht völlig abschalten.

Es besteht ein Zusammenhang zwischen dem ungestörten clientseitigen Ablauf bzw.

einem durch z.B. eine Cookie-Rückfrage unterbrochenen Ablauf und dem Auftreten des

Problems. Es besteht ein Zusammenhang zwischen Plattform des Client und dem Auftreten

des Bug. Unter Linux und Windows NT wechselt die Einschlagstelle von Aufruf zu Aufruf.

Auf Apple Macintosh dagegen ist die Einschlagstelle konstant.

Das Problem tritt aber merkwürdigerweise nur dann auf, wenn der Content via CGI erzeugt wird, nicht jedoch, wenn der selbe Content aus einer statischen HTML-Datei stammt. Ein Zusammenhang mit dem Header konnte nicht nachgewiesen werden.

Ein Zusammenhang mit den cgi-Namen (z.B. Dateierdung) konnte auch nicht nachgewiesen werden.

Wird die statische HTML-Datei durch ein PHP-Script geliefert, dann tritt auch kein Fehler auf. Auch die Ausgabe der gleichen Header wie im cgi kann den Fehler nicht reproduzieren.

Content-Type: text/html

Connection: close

gmL-Modul-Version: 2.0.0 build: -2.00310 Mon Mär 12 22:21:36 MET 2001  
compiled@granne

Content-Length: 36883

Der Test erfolgt durch Eintippen der URL. Sobald die Seite komplett geladen ist wird Relod gedrückt. Jetzt ist sie defekt. Nach erneuten Reload ist sie je nach Cache-Einstellung unterschiedlich of ebenfalls defekt oder wieder in

Ordnung. Eine Vorhersage, wann ein Reload zu einer defekten Seite und wann es

zu einer fehlerfreien Seite führt, ist nicht möglich.

***Fri, 23 Mar 2001 18:42:38***

[<3ABB8B0E.7060003@bioshop.de>](mailto:3ABB8B0E.7060003@bioshop.de)

Noch ein Merkwürden:

Wenn ich NN4 so konfiguriere, daß er mich vor Keksen warnen soll, dann

tritt der Bug nicht auf, sobald NN4 durch einen Keks unterbrochen wird und die Warnung anzeigt. Lehne ich dagegen Kekse ab, oder nehme ich Kekse ohne Rückfrage an, dann kann er wieder ungestört seinen Mist machen.

Diese Spielart wurde mit NN4.7 unter Linux beobachtet.

Unter Linux und NT ändern sich die Einschlagstellen von Aufruf zu Aufruf. Auf dem Mac dagegen ist die Einschlagstelle konstant.

Gruß, Georg

---