

## [VulnWatch] pacsec hype security team: 7 words of warning about Macromedia Flash Player 9+

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-10/msg00004.html>

---

- *From:* Dragos Ruiu <[dr@xxxxxxx](mailto:dr@xxxxxxx)>
  - *Date:* Tue, 10 Oct 2006 14:41:05 -0700
- 

Advisory:

"The new Flash player adds network functions!"

Details:

With a minor amount of fanfare "binary socket" support has been added to Flash Player 9 / ActionScript 3.0. The Flash sandbox model is primarily focused on preventing modifications to the local system, and thus there are many ways to bypass the only-connect-back-upstream and port<1024 limitations on the SWF applet Socket() class. A (potentially malicious) server can override the limit with a cross domain policy file on the server, or it can be overridden locally at the player with a global setting/policy change, or by configuring the applet as trusted.

Adobe has a paper on flash security configuration at:  
[http://www.adobe.com/devnet/flashplayer/articles/flash\\_player\\_9\\_security.pdf](http://www.adobe.com/devnet/flashplayer/articles/flash_player_9_security.pdf)

The potential for network misuse possible in Flash just went up several orders of magnitude, and as the Adobe site triumphantly proclaims, it's apparently in use at 97.3% of networked computers. I'll avoid some of the more exotic scenarios, lest they give anyone some bad ideas – and leave this caveat at this warning.

Audited the trusted Flash applets on your system lately?

Forewarned is Forearmed.

cheers,  
--dr

—

World Security Pros. Cutting Edge Training, Tools, and Techniques  
Tokyo, Japan November 27–30 2006 <http://pacsec.jp>  
pgpkey <http://dragos.com/> kyxpgp