```
     _____   _____      _____
     \     \   \     \\      \     \    /     /
     /  |   \/  ___\//   __\/      \   /  _____ ___  ___
    /   |    \     \___\    \__     \   \_\   \ |  \( <_> )   |  / |> >
    \___|__  /\_____ /\____  /   _____\/_|   \____/|___/|__/
           \/       \/       \/        \/              |__|
```

~.
Vulnerability Summary
~.

Title   Adobe flash sandbox bypass to navigate to local drives
Release Date   12 August 2014
Reference   NGS00711
Discoverer   Soroush Dalili
Vendor   Adobe
Vendor Reference PSIRT-2823
Systems Affected Flash Player 14.0.0.125 (tested with IE 11)
CVE Reference   CVE-2014-0541
Risk   Medium
Status   Fixed

~.
Resolution Timeline
~.

Discovered   10 June 2014
Reported   10 June 2014
Released   10 June 2014
Fixed   12 August 2014
Published   12 August 2014

~.
Vulnerability Description
~.

It is possible to bypass the Adobe Flash security sandbox and browse files on the
local drives. The attack has been confirmed in Microsoft IE 11, although it may
also work with other browsers.

~.
Technical Details
~.

In order to replicate the issue, browse to the following URL:
http://website/page.swf?input=\\/c:/
This will display the contents of the C drive.

The issue is within the following function:
navigateToURL(new URLRequest(root.loaderInfo.parameters.input),"_self");

The attack can also be achieved in other browsers, but as some (e.g. Google Chrome)
have their own protection mechanisms, even bypassing the Flash sandbox does not
result in access to the local drives.

~.
Fix Information
~.

A patch can be downloaded from the following location:
http://helpx.adobe.com/security/products/flash-player/apsb14-18.html

~.
NCC Group
~.