



eSecurity Advisory Adobe Flash Player Exploit

A vulnerability has been discovered in earlier versions of **Adobe Flash Player** that could allow a remote attacker to run and execute commands on the local system or cause a Denial of Service. Currently, this vulnerability is being exploited on a number of websites.

This vulnerability does not affect the most recent version of Adobe Flash Player (9.0.124.0). Analysis has revealed that this vulnerability is related to the flaw discovered by Mark Dowd of IBM in April 2008. This vulnerability is a variant of CVE-2007-0071. The sites involved in these attacks are using the same exploit, but the payloads are known to vary with varying rates of anti-virus detection. Links to these exploit sites are being injected into third-party sites through SQL-injection vulnerabilities.

What can you do?

We recommend the following actions be taken immediately:

- Upgrade your Adobe Flash Player to the [latest version](#) (9.0.124.0) for each web browser you use (Internet Explorer, Safari, Firefox, etc.).
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Ensure that all anti-virus software is up to date with the latest signatures. We recommend that signatures are updated daily.

SOFTWARE AFFECTED:

- Adobe Flash Player 9.0.115.0 and earlier
- Flash CS3 Professional
- Flash Professional 8
- Flash Basic
- Flex 3.0
- AIR 1.0

REFERENCES:

Adobe:

http://blogs.adobe.com/psirt/2008/05/potential_flash_player_issue.html

SecurityFocus:

<http://www.securityfocus.com/bid/29386>

<http://www.securityfocus.com/bid/28695>

eSecurity Advisory: Adobe Flash Player Exploit

Delaware Department of Technology and Information

May 29, 2008

Symantec:

http://www.symantec.com/security_response/threatcon/index.jsp

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0071>

Mark Dowd:

http://documents.iss.net/whitepapers/IBM_X-Force_WP_final.pdf

Compiled in part from:

MS-ISAC

30 South Pearl Street, Suite P2

Albany, NY 12207

(518) 474-0865

7x24 MS-ISAC Operational Center 1-866-787-4722