

[GLSA 200903-23] Adobe Flash Player: Multiple vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2009-03/msg00113.html>

- *From:* Pierre-Yves Rofes <py@xxxxxxxxxxx>
 - *Date:* Tue, 10 Mar 2009 23:27:02 +0100
-

Gentoo Linux Security Advisory GLSA 200903-23

<http://security.gentoo.org/>

Severity: Normal
Title: Adobe Flash Player: Multiple vulnerabilities
Date: March 10, 2009
Bugs: #239543, #251496, #260264
ID: 200903-23

Synopsis

=====

Multiple vulnerabilities have been identified, the worst of which allow arbitrary code execution on a user's system via a malicious Flash file.

Background

=====

The Adobe Flash Player is a renderer for the popular SWF file format, which is commonly used to provide interactive websites, digital experiences and mobile content.

Affected packages

=====

Package / Vulnerable / Unaffected

1 net-www/netscape-flash < 10.0.22.87 >= 10.0.22.87

Description

=====

Multiple vulnerabilities have been discovered in Adobe Flash Player:

- * The access scope of `System.setClipboard()` allows ActionScript programs to execute the method without user interaction (CVE-2008-3873).
- * The access scope of `FileReference.browse()` and `FileReference.download()` allows ActionScript programs to execute the methods without user interaction (CVE-2008-4401).
- * The Settings Manager controls can be disguised as normal graphical elements. This so-called "clickjacking" vulnerability was disclosed by Robert Hansen of SecTheory, Jeremiah Grossman of WhiteHat Security, Eduardo Vela, Matthew Mastracci of DotSpots, and Liu Die Yu of TopsecTianRongXin (CVE-2008-4503).
- * Matthew Dempsky reported a null-pointer dereference flaw when loading two SWF files compiled with different Flash versions from the same URI (CVE-2008-4546).
- * Adan Barth (UC Berkely) and Collin Jackson (Stanford University) discovered a flaw occurring when interpreting HTTP response headers (CVE-2008-4818).
- * Nathan McFeters and Rob Carter of Ernst and Young's Advanced Security Center are credited for finding an unspecified vulnerability facilitating DNS rebinding attacks (CVE-2008-4819).
- * When used in a Mozilla browser, Adobe Flash Player does not properly interpret jar: URLs, according to a report by Gregory Fleischer of pseudo-flaw.net (CVE-2008-4821).
- * Alex "kuza55" K. reported that Adobe Flash Player does not properly interpret policy files (CVE-2008-4822).
- * The vendor credits Stefano Di Paola of Minded Security for reporting that an ActionScript attribute is not interpreted properly (CVE-2008-4823).
- * Riley Hassell and Josh Zelonis of iSEC Partners reported multiple input validation errors (CVE-2008-4824).
- * The aforementioned researchers also reported that ActionScript 2 does not verify a member element's size when performing several known and other unspecified actions, that `DefineConstantPool` accepts an untrusted input value for a "constant count" and that character elements are not validated when retrieved from a data structure, possibly resulting in a null-pointer dereference (CVE-2008-5361, CVE-2008-5362, CVE-2008-5363).
- * The vendor reported an unspecified arbitrary code execution

vulnerability (CVE-2008-5499).

* Liu Die Yu of TopsecTianRongXin reported an unspecified flaw in the Settings Manager related to "clickjacking" (CVE-2009-0114).

* The vendor credits Roe Hay from IBM Rational Application Security for reporting an input validation error when processing SWF files (CVE-2009-0519).

* Javier Vicente Vallejo reported via the iDefense VCP that Adobe Flash does not remove object references properly, leading to a freed memory dereference (CVE-2009-0520).

* Josh Bressers of Red Hat and Tavis Ormandy of the Google Security Team reported an untrusted search path vulnerability (CVE-2009-0521).

Impact

=====

A remote attacker could entice a user to open a specially crafted SWF file, possibly resulting in the execution of arbitrary code with the privileges of the user or a Denial of Service (crash). Furthermore a remote attacker could gain access to sensitive information, disclose memory contents by enticing a user to open a specially crafted PDF file inside a Flash application, modify the victim's clipboard or render it temporarily unusable, persuade a user into uploading or downloading files, bypass security restrictions with the assistance of the user to gain access to camera and microphone, conduct Cross-Site Scripting and HTTP Header Splitting attacks, bypass the "non-root domain policy" of Flash, and gain escalated privileges.

Workaround

=====

There is no known workaround at this time.

Resolution

=====

All Adobe Flash Player users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=net-www/netscape-flash-10.0.22.87"
```

References

=====

[1] CVE-2008-3873
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3873>
[2] CVE-2008-4401
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4401>

[GLSA 200903-23] Adobe Flash Player: Multiple vulnerabilities

- [3] CVE-2008-4503
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4503>
- [4] CVE-2008-4546
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4546>
- [5] CVE-2008-4818
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4818>
- [6] CVE-2008-4819
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4819>
- [7] CVE-2008-4821
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4821>
- [8] CVE-2008-4822
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4822>
- [9] CVE-2008-4823
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4823>
- [10] CVE-2008-4824
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4824>
- [11] CVE-2008-5361
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5361>
- [12] CVE-2008-5362
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5362>
- [13] CVE-2008-5363
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5363>
- [14] CVE-2008-5499
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5499>
- [15] CVE-2009-0114
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0114>
- [16] CVE-2009-0519
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0519>
- [17] CVE-2009-0520
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0520>
- [18] CVE-2009-0521
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0521>

Availability
=====

This GLSA and any updates to it are available for viewing at the Gentoo Security Website:

<http://security.gentoo.org/glsa/glsa-200903-23.xml>

Concerns?
=====

Security is a primary focus of Gentoo Linux and ensuring the confidentiality and security of our users machines is of utmost importance to us. Any security concerns should be addressed to security@xxxxxxxxxx or alternatively, you may file a bug at <http://bugs.gentoo.org>.

License

=====

Copyright 2009 Gentoo Foundation, Inc; referenced text belongs to its owner(s).

The contents of this document are licensed under the Creative Commons – Attribution / Share Alike license.

<http://creativecommons.org/licenses/by-sa/2.5>

*Attachment: **signature.asc***

Description: OpenPGP digital signature