

[Full-disclosure] [GLSA 200805-18] Mozilla products: Multiple vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-05/msg00510.html>

- *From:* Robert Buchholz <rbu@xxxxxxxxxxx>
 - *Date:* Tue, 20 May 2008 23:18:23 +0200
-

Gentoo Linux Security Advisory GLSA 200805-18

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

Severity: Normal
Title: Mozilla products: Multiple vulnerabilities
Date: May 20, 2008
Bugs: #208128, #214816, #218065
ID: 200805-18

Synopsis

=====

Multiple vulnerabilities have been reported in Mozilla Firefox, Thunderbird, SeaMonkey and XULRunner, some of which may allow user-assisted execution of arbitrary code.

Background

=====

Mozilla Firefox is an open-source web browser and Mozilla Thunderbird an open-source email client, both from the Mozilla Project. The SeaMonkey project is a community effort to deliver production-quality releases of code derived from the application formerly known as the 'Mozilla Application Suite'. XULRunner is a Mozilla runtime package that can be used to bootstrap XUL+XPCOM applications like Firefox and Thunderbird.

Affected packages

=====

Package / Vulnerable / Unaffected

- 1 mozilla-firefox < 2.0.0.14 >= 2.0.0.14
- 2 mozilla-firefox-bin < 2.0.0.14 >= 2.0.0.14
- 3 mozilla-thunderbird < 2.0.0.14 >= 2.0.0.14
- 4 mozilla-thunderbird-bin < 2.0.0.14 >= 2.0.0.14
- 5 seamonkey < 1.1.9-r1 >= 1.1.9-r1
- 6 seamonkey-bin < 1.1.9 >= 1.1.9
- 7 xulrunner < 1.8.1.14 >= 1.8.1.14

7 affected packages on all of their supported architectures.

Description

=====

The following vulnerabilities were reported in all mentioned Mozilla products:

- * Jesse Ruderman, Kai Engert, Martijn Wargers, Mats Palmgren, and Paul Nickerson reported browser crashes related to JavaScript methods, possibly triggering memory corruption (CVE-2008-0412).
- * Carsten Book, Wesley Garland, Igor Bukanov, moz_bug_r_a4, shutdown, Philip Taylor, and tgirmann reported crashes in the JavaScript engine, possibly triggering memory corruption (CVE-2008-0413).
- * David Bloom discovered a vulnerability in the way images are treated by the browser when a user leaves a page, possibly triggering memory corruption (CVE-2008-0419).
- * moz_bug_r_a4, Boris Zbarsky, and Johnny Stenback reported a series of privilege escalation vulnerabilities related to JavaScript (CVE-2008-1233, CVE-2008-1234, CVE-2008-1235).
- * Mozilla developers identified browser crashes caused by the layout and JavaScript engines, possibly triggering memory corruption (CVE-2008-1236, CVE-2008-1237).
- * moz_bug_r_a4 and Boris Zbarsky discovered that pages could escape from its sandboxed context and run with chrome privileges, and inject script content into another site, violating the browser's same origin policy (CVE-2008-0415).
- * Gerry Eisenhaur discovered a directory traversal vulnerability when using "flat" addons (CVE-2008-0418).
- * Alexey Proskuryakov, Yosuke Hasegawa and Simon Montagu reported multiple character handling flaws related to the backspace character, the "0x80" character, involving zero-length non-ASCII sequences in multiple character sets, that could facilitate Cross-Site Scripting attacks (CVE-2008-0416).

The following vulnerability was reported in Thunderbird and SeaMonkey:

* regenrecht (via iDefense) reported a heap-based buffer overflow when rendering an email message with an external MIME body (CVE-2008-0304).

The following vulnerabilities were reported in Firefox, SeaMonkey and XULRunner:

* The fix for CVE-2008-1237 in Firefox 2.0.0.13 and SeaMonkey 1.1.9 introduced a new crash vulnerability (CVE-2008-1380).

* hong and Gregory Fleischer each reported a variant on earlier reported bugs regarding focus shifting in file input controls (CVE-2008-0414).

* Gynvael Coldwind (Vexillum) discovered that BMP images could be used to reveal uninitialized memory, and that this data could be extracted using a "canvas" feature (CVE-2008-0420).

* Chris Thomas reported that background tabs could create a borderless XUL pop-up in front of pages in other tabs (CVE-2008-1241).

* oo.rio.oo discovered that a plain text file with a "Content-Disposition: attachment" prevents Firefox from rendering future plain text files within the browser (CVE-2008-0592).

* Martin Straka reported that the ".href" property of stylesheet DOM nodes is modified to the final URI of a 302 redirect, bypassing the same origin policy (CVE-2008-0593).

* Gregory Fleischer discovered that under certain circumstances, leading characters from the hostname part of the "Referer:" HTTP header are removed (CVE-2008-1238).

* Peter Brodersen and Alexander Klink reported that the browser automatically selected and sent a client certificate when SSL Client Authentication is requested by a server (CVE-2007-4879).

* Gregory Fleischer reported that web content fetched via the "jar:" protocol was not subject to network access restrictions (CVE-2008-1240).

The following vulnerabilities were reported in Firefox:

* Justin Dolske discovered a CRLF injection vulnerability when storing passwords (CVE-2008-0417).

* Michal Zalewski discovered that Firefox does not properly manage a delay timer used in confirmation dialogs (CVE-2008-0591).

* Emil Ljungdahl and Lars-Olof Moilanen discovered that a web forgery warning dialog is not displayed if the entire contents of a web page are in a DIV tag that uses absolute positioning (CVE-2008-0594).

Impact

=====

A remote attacker could entice a user to view a specially crafted web page or email that will trigger one of the vulnerabilities, possibly leading to the execution of arbitrary code or a Denial of Service. It is also possible for an attacker to trick a user to upload arbitrary files when submitting a form, to corrupt saved passwords for other sites, to steal login credentials, or to conduct Cross-Site Scripting and Cross-Site Request Forgery attacks.

Workaround

=====

There is no known workaround at this time.

Resolution

=====

All Mozilla Firefox users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask -1 -v ">=www-client/mozilla-firefox-2.0.0.14"
```

All Mozilla Firefox binary users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask -1 -v ">=www-client/mozilla-firefox-bin-2.0.0.14"
```

All Mozilla Thunderbird users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask -1 -v ">=mail-client/mozilla-thunderbird-2.0.0.14"
```

All Mozilla Thunderbird binary users should upgrade to the latest version:

```
# emerge --sync
# emerge -a -1 -v ">=mail-client/mozilla-thunderbird-bin-2.0.0.14"
```

All SeaMonkey users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask -1 -v ">=www-client/seamonkey-1.1.9-r1"
```

All SeaMonkey binary users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask -1 -v ">=www-client/seamonkey-bin-1.1.9"
```

All XULRunner users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=net-libs/xulrunner-1.8.1.14"
```

NOTE: The crash vulnerability (CVE-2008-1380) is currently unfixed in the SeaMonkey binary ebuild, as no precompiled packages have been released. Until an update is available, we recommend all SeaMonkey users to disable JavaScript, use Firefox for JavaScript-enabled browsing, or switch to the SeaMonkey source ebuild.

References

=====

- [1] CVE-2007-4879
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4879>
- [2] CVE-2008-0304
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0304>
- [3] CVE-2008-0412
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0412>
- [4] CVE-2008-0413
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0413>
- [5] CVE-2008-0414
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0414>
- [6] CVE-2008-0415
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0415>
- [7] CVE-2008-0416
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0416>
- [8] CVE-2008-0417
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0417>
- [9] CVE-2008-0418
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0418>
- [10] CVE-2008-0419
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0419>
- [11] CVE-2008-0420
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0420>
- [12] CVE-2008-0591
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0591>
- [13] CVE-2008-0592
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0592>
- [14] CVE-2008-0593
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0593>
- [15] CVE-2008-0594
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0594>
- [16] CVE-2008-1233
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1233>
- [17] CVE-2008-1234

[Full-disclosure] [GLSA 200805-18] Mozilla products: Multiple vulnerabilities

- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1234>
[18] CVE-2008-1235
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1235>
[19] CVE-2008-1236
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1236>
[20] CVE-2008-1237
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1237>
[21] CVE-2008-1238
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1238>
[22] CVE-2008-1240
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1240>
[23] CVE-2008-1241
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1241>
[24] CVE-2008-1380
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1380>

Availability

=====

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

<http://security.gentoo.org/glsa/glsa-200805-18.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 2008 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: This is a digitally signed message part.

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>