Google Chrome Multiple Vulnerabilities

2012-05-25 02:06:22 by Raven

SECUNIA ADVISORY ID: SA49277

VERIFY ADVISORY: Secunia.com http://secunia.com/advisories/49277/

RELEASE DATE: 2012-05-24

CRITICALITY: **Highly Critical**

DESCRIPTION: Multiple vulnerabilities have been reported in Google Chrome, where some have unknown impacts and others can be exploited by malicious people to compromise a user's system. The vulnerabilities are reported in versions prior to 19.0.1084.52.
1) An unspecified error exists in the v8 garbage collection, which may result in a crash.
2) An out-of-bounds read error exists in Skia.
3) A use-after-free error exists in first-letter handling.
4) An error with websockets over SSL can be exploited to corrupt memory.
5) An unspecified error exists in the plug-in JavaScript bindings, which may result in a crash.
6) A use-after-free error exists in the browser cache.
7) A bad cast error exists in the GTK UI.
8) Some errors in the PDF handling can be exploited to cause out-of-bounds writes.
9) An invalid read error exists in v8.
10) A use-after-free error exists with encrypted PDF.
11) An invalid cast error exists with colorspace handling in PDF.
12) An error with PDF functions can be exploited to cause a buffer overflow.
13) A type corruption error exists in v8.

SOLUTION: Update to version 19.0.1084.52.

PROVIDED AND/OR DISCOVERED BY: The vendor credits:
1) Brett Wilson, Chromium development community.
2) Inferno, Google Chrome Security Team.
3) miaubiz.
4, 5) Dharani Govindan, Chromium development community.
6) efbiaiinzinz.
7) Micha Bartholome.
8, 10-11) Mateusz Jurczyk, Google Security Team and Gynvael Coldwind, Google Security Team.
9, 13) Christian Holler.
12) scarybeasts, Google Chrome Security Team.

ORIGINAL ADVISORY: http://googlechromereleases.blogspot.com/2012/05/stable-channel-update_23.html