Mozilla Roll-out: Firefox 0.9.3, Mozilla Suite 1.7.2 and Mozilla Thunderbird 0.7.3 are available, fixes serious security issues.

The new version closes 4 security flaws: A CA certificate DoS, an exploit in the Windows version that allows attackers to run evil code, a libpng bug and a flaw allowing sites to falsely claim they are using a secure ssl connection.

1. New Versions
2. Open Source with it's pants down
3. Consider upgrading libpng
4. Engineer skills required v.s. Windows Update

1. New Versions

New versions of the the award winning Mozilla browser products are available:

- **Mozilla Suite 1.7.2** is a Internet application suite featuring the Mozilla browser, a sophisticated e-mail and newsgroup client, a dull IRC chat client, and a frontpage-like simple HTML editor and a schedule calendar (new from 1.6). Luckily the individual parts are ./configure flags on Linux, you are free not to compile the less elegant parts of the (huge) package. The browser uses the **Gecko** rendering engine to show pages.
- **Firefox 0.9.3** also uses **Gecko**, but has a totally different graphical user interface. Firefox is becoming extremely popular and may already be the worlds most used browser. Like Mozilla, Epiphany, Galeon and other Gecko browsers, Firefox does demand modern hardware. Users with older hardware are probably better off using **Opera**.
- **Mozilla Thunderbird 0.7.3** is a powerfull email client with imap (and pop3) support. Most of Thunderbird is, like Firefox, based on Mozilla. And the graphical user interface is, like Firefox, excellent.

2. Open Source with it's pants down

The new releases fixes **four security flaws**:

- bug 249004, "Importing false CA certificate leading to error -8182 (perm DoS), especially exploitabe by email"
This vulnerability is present in Linux as well as Windows. It has been found present on Mozilla 1.6 and 1.7 on Debian 3.0 stable.

Actual Results: Mozilla imports the "forged" root cert into the "authorities" tab of the cert manager as an untrusted root. You can identify it by the column "security device": it is stored in the "software security device" instead of the "Builtin Object Token". However, your certificate store is "corrupted" from this time on: open a website protected by an SSL certificate signed by the root CA cert you've been forging (e.g. https://www.thawte.com/) and you'll get an error -8182.

Conclusion: fully automatic DoS of the entire cert store via email is possible, no user interaction needed.

bug 250906 is a serious two-part Windows-only bug.

1. Firefox stores the cache data in a known location. There are 3 files in that folder has known names, _CACHE_001_, _CACHE_002_, and _CACHE_003_.
2. %00 allows you to end a filename, _CACHE_001_%00.html would ask for CACHE_001_.

You visit a website. The extraordinary evil web-master places naughty javascript code in your cache, then

- finds a way to redirect you to a carefully crafted file:// location. Now you're owned and the evil person has control of your computer, bank accounts and so forth.

bug 251381 is a problem in libpng-1.2.5 and earlier. The Mozilla Windows binary has libpng build-in, meaning the whole browser must be replaced. Most Linux distributions have made safe libpng packages available.

bug 253121, (CAN-2004-0763), "lock icon and certificates spoofable with onunload document.write", is a minor bug that allows a website to appear to be using ssl by showing the secure connection icon.

3. Consider upgrading libpng

Safe libpng packages for SuSE Linux were made available Wednesday, Aug 4th 2004 16:00 MEST. From their security list:

1) problem description, brief discussion

Several different security vulnerabilities were found in the PNG library which is used by applications to support the PNG image format.

A remote attacker is able to execute arbitrary code by triggering a buffer overflow due to the incorrect handling of the length of transparency chunk data and in other pathes of image processing. (VU#388984, VU#817368, CAN-2004-0597)

A special PNG image can be used to cause an application crashing due to NULL pointer dereference in the function png_handle_iCPP() (and other locations). (VU#236656, CAN-2004-0598)

Integer overflows were found in png_handle_sPLT(), png_read_png() functions and other locations. These bugs may at least crash an application. (VU#160448, VU#477512, VU#286464, CAN-2004-0599)

Many thanks to Chris Evans who reported issues to us and other vendors.

- Read the full SUSE Security Announcement SUSE SA_2004_023
- Gentoo Linux made safe libpng packages available 2004-08-15.
Trustix Linux made safe libpng packages available 2004-08-15.

• Check your distributions homepage and/or bugzilla to find your distributions libpng status.

NOT fixed in this release, enjoy:

• bug 22183, "UI spoofing can cause user to mistake content for chrome." It can be hard to tell who you are voting for, interfaces can be misleading. You can still become a victim of window spoofing. It has been demonstrated how someone can create a fake location bar on top of your current location bar and thereby know what websites you want to visit. Chances are high that may be abused more seriously.

• bug 154892, Splitting Absolutely positioned frames not implemented, Missing second page of content when printing or print previewing this, OPEN SINCE 2002!

4. Engineer skills required v.s. Windows Update

Windows users worldwide are slightly upset because of the upgrade procedure. Windows users must make sure they uninstall Mozilla and/or Firefox before installing the new version. You can't just apply a small patch, the whole browser must be replaced. Some claim Windows Update is so much better because a few of the many updates are smaller. The upgrade to Firefox 0.9.2 was a small XML file patch, this time Firefox users must download the complete 5M browser binary, uninstall and reinstall. Installing over the top of an older version may cause unpredictable problems. (bug 237727)

The new versions are available at http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/0.9.3/

Firefox 0.9.3 was added to the Gentoo Portage tree 2004-08-05.

Related reading:

• MozillaZine: Firefox, Thunderbird, Mozilla Suite Upgrades Released
• The secrets of Mozilla 1.6+ and Firefox 9.x