

Multiple vulnerabilities in Mozilla products

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-11/4289.html>

From: JM Tella Llop [MVP Windows] (*jmtella_at_XXXmvps.org*)

Date: 11/06/04

Date: Sat, 6 Nov 2004 19:37:56 +0100

Multiple vulnerabilities in Mozilla products

Original release date: September 17, 2004

Last revised: ---

Source: US-CERT

Systems Affected

Mozilla software, including the following:

- * Mozilla web browser, email and newsgroup client
- * Firefox web browser
- * Thunderbird email client

Overview

Several vulnerabilities exist in the Mozilla web browser and derived products, the most serious of which could allow a remote attacker to execute arbitrary code on an affected system.

I. Description

Several vulnerabilities have been reported in the Mozilla web browser and derived products. More detailed information is available in the individual vulnerability notes:

VU#414240 – Mozilla Mail vulnerable to buffer overflow via writeGroup() function in nsVCardObj.cpp

Mozilla Mail contains a stack overflow vulnerability in the display routines for VCards. By sending an email message with a crafted VCard, a remote attacker may be able to execute arbitrary code on the victim's machine with the privileges of the current user. This can be exploited in the preview mode as well.

VU#847200 – Mozilla contains integer overflows in bitmap image decoder

A vulnerability in the way Mozilla and its derived programs handle certain bitmap images could allow a remote attacker to execute arbitrary code on a vulnerable system.

microsoft.public.windowsxp.general: Multiple vulnerabilities in Mozilla products

VU#808216 – Mozilla contains heap overflow in UTF8 conversion of hostname portion of URLs

A vulnerability in the way Mozilla and its derived programs handle certain malformed URLs could allow a remote attacker to execute arbitrary code on a vulnerable system.

VU#125776 – Multiple buffer overflows in Mozilla POP3 protocol handler

There are multiple buffer overflow vulnerabilities in the Mozilla POP3 protocol handler that could allow a malicious POP3 server to execute arbitrary code on the affected system.

VU#327560 – Mozilla "send page" feature contains a buffer overflow vulnerability

There is a buffer overflow vulnerability in the Mozilla "send page" feature that could allow a remote attacker to execute arbitrary code.

VU#651928 – Mozilla allows arbitrary code execution via link dragging

A vulnerability affecting Mozilla web browsers may allow violation of cross-domain scripting policies and possibly execute code originating from a remote source.

II. Impact

These vulnerabilities could allow a remote attacker to execute arbitrary code with the privileges of the user running the affected application.

VU#847200 could also allow a remote attacker to crash an affected application.

III. Solution

Upgrade to a patched version

Mozilla has released versions of the affected software that contain patches for these issues:

- * Mozilla 1.7.3
- * Firefox Preview Release
- * Thunderbird 0.8

Users are strongly encouraged to upgrade to one of these versions.

Appendix A. References

- * Mozilla Security Advisory – <http://www.mozilla.org/projects/security/known-vulnerabilities.html>
- * Mozilla 1.7.2 non-ascii hostname heap overrun, Gaël Delalleau – <http://www.zencomsec.com/advisories/mozilla-1.7.2-UTF8link.txt>
- * Security Audit of Mozilla's .bmp image parsing, Gaël Delalleau –

microsoft.public.windowsxp.general: Multiple vulnerabilities in Mozilla products

<<http://www.zencomsec.com/advisories/mozilla-1.7.2-BMP.txt>>
* Security Audit of Mozilla's POP3 client protocol, Gaël Delalleau
– <<http://www.zencomsec.com/advisories/mozilla-1.7.2-POP3.txt>>
* US-CERT Vulnerability Note VU#414240 –
<<http://www.kb.cert.org/vuls/id/414240>>
* US-CERT Vulnerability Note VU#847200 –
<<http://www.kb.cert.org/vuls/id/847200>>
* US-CERT Vulnerability Note VU#808216 –
<<http://www.kb.cert.org/vuls/id/808216>>
* US-CERT Vulnerability Note VU#125776 –
<<http://www.kb.cert.org/vuls/id/125776>>
* US-CERT Vulnerability Note VU#327560 –
<<http://www.kb.cert.org/vuls/id/327560>>
* US-CERT Vulnerability Note VU#651928 –
<<http://www.kb.cert.org/vuls/id/651928>>

Mozilla has assigned credit for reporting of these issue to the following:

- * VU#414240: Georgi Guninski
- * VU#847200: Gaël Delalleau
- * VU#808216: Gaël Delalleau and Mats Palmgren
- * VU#125776: Gaël Delalleau
- * VU#327560: Georgi Guninski
- * VU#651928: Jesse Ruderman

Feedback can be directed to the US-CERT Technical Staff.

Copyright 2004 Carnegie Mellon University. Terms of use

Revision History

Sep 17, 2004: Initial release

--

Jose Manuel Tella Llop

MVP – Windows

jmtella@XXXcompuserve.com (quitar XXX)

<http://www.multingles.net/jmt.htm>

Este mensaje se proporciona "como está" sin garantías de ninguna clase, y no otorga ningún derecho.

This posting is provided "AS IS" with no warranties, and confers no rights.

You assume all risk for your use.