

# Re: US-CERT Technical Cyber Security Alert TA04-261A -- Multiple vulnerabilities in Mozilla products

**Source:**

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.basics/2004-09/3424.html>

---

**From:** Herb Fritatta (*Herb\_at\_nospam.com*)

**Date:** 09/19/04

Date: Sun, 19 Sep 2004 18:52:09 -0500

David H. Lipman wrote:

> -----BEGIN PGP SIGNED MESSAGE-----  
> Hash: SHA1  
>  
> *Technical Cyber Security Alert TA04-261A*  
> *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.*
- >
- > *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>>
- > *ml*
- > \* *Mozilla 1.7.2 non-ascii hostname heap overrun, Gael Delalleau –*
- > <<http://www.zencomsec.com/advisories/mozilla-1.7.2-UTF8link.txt>>
- > \* *Security Audit of Mozilla's .bmp image parsing, Gael Delalleau –*
- > <<http://www.zencomsec.com/advisories/mozilla-1.7.2-BMP.txt>>
- > \* *Security Audit of Mozilla's POP3 client protocol, Gael 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: Gael Delalleau*
- > \* *VU#808216: Gael Delalleau and Mats Palmgren*
- > \* *VU#125776: Gael Delalleau*
- > \* *VU#327560: Georgi Guninski*
- > \* *VU#651928: Jesse Ruderman*
- >
- > \_\_\_\_\_
- >
- > *Feedback can be directed to the US-CERT Technical Staff.*
- >
- > \_\_\_\_\_
- >
- > *This document is available from:*
- >
- > <<http://www.us-cert.gov/cas/techalerts/TA04-261A.html>>

>  
> \_\_\_\_\_  
>  
> Copyright 2004 Carnegie Mellon University.  
>  
> Terms of use: <<http://www.us-cert.gov/legal.html>>  
> \_\_\_\_\_  
>  
> Revision History  
>  
> Sept 17, 2004: Initial release  
>  
> -----BEGIN PGP SIGNATURE-----  
> Version: GnuPG v1.2.1 (GNU/Linux)  
>  
> iQEVAwUBQUtEPBhoSezw4YfQAQIosQgAkny8jByUHOSsukYr4u20BGhOb1FI2wKY  
> GilIzIJy8sKtHq6S3XHMK5xXH8dDgheODPV3NLB6X6sksG4x1o5pQKq2lgANas13  
> EIlfVb5p3//uS0qV/zhPlc7tkBcJAVgx1BaExorJpsHeEfhF22+hPt+BuuBM875B  
> TlowipQIGbADQjhh4zVAJYSsLl3R8ZHYu8QnJlRn+qCF2Psg2eTnXlzfzIHvhl/3  
> KuaeqQ86V+B+uXUox2FjlrOzYujUY2z+syRkfNFINIo3E51rRjxF5SGxNt0gPD+y  
> CqZw4LDf+HqdpIQd6J/vJq4GcOkOXYraXskUK8zwCiSwqSw1ucYGvA==  
> =CIIN  
> -----END PGP SIGNATURE-----  
>  
>  
>

And your point is???