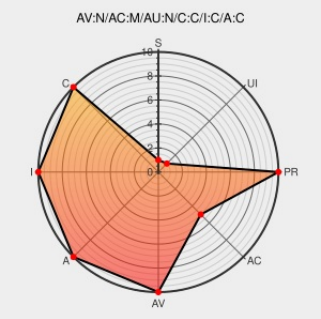
CVE-2010-1028

Published on: 03/19/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:04 PM UTC

CVE-2010-1028

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows Vista from Microsoft contain the following vulnerability:

Integer overflow in the decompression functionality in the Web Open Fonts Format (WOFF) decoder in Mozilla Firefox 3.6 before 3.6.2 and 3.7 before 3.7 alpha 3 allows remote attackers to execute arbitrary code via a crafted WOFF file that triggers a buffer overflow, as demonstrated by the vd_ff module in VulnDisco 9.0.

CVE-2010-1028 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
US-CERT Vulnerability Note VU#964549	US Government Resource, www.kb.cert.org, text/html	CERT-VN VU#964549
Immunity Forum	web.archive.org, text/html, Inactive Link, Not Archived	MISC forum.immunityinc.com/board/thread/1161/vulndisco-9-0/
Zero day exploit for Firefox 3.6 - The H Security: News and Features	www.h-online.com, text/html	MISC www.h-online.com/security/news/item/Zero-day-exploit-for-Firefox-3-6-936124.html
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:7969
Secunia Advisory SA38608 at Mozilla Security	blog.mozilla.com	MISC blog.mozilla.com/security/2010/02/22/secunia-

Blog	text/html	advisory-sa38608/
Bug 552216 – WOFF heap corruption due to integer overflow	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=552216
About Secunia Research | Flexera	Vendor Advisory web.archive.org text/html	SECUNIA 38608
About Secunia Research | Flexera	Vendor Advisory web.archive.org text/html	MISC secunia.com/community/forum/thread/show/3592
Update on Secunia Advisory SA38608 at Mozilla Security Blog	blog.mozilla.com text/html	CONFIRM blog.mozilla.com/security/2010/03/18/update-on-secunia-advisory-sa38608/
Going Commercial with Firefox Vulnerabilities | Klipper on Security	blog.psi2.de text/html	MISC blog.psi2.de/en/2010/02/20/going-commercial-with-firefox-vulnerabilities/
MFSA 2010-08: WOFF heap corruption due to integer overflow	Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/2010/mfsa2010-08.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows Vista	All	All	All	All
Operating System	Microsoft	Windows Vista	All	All	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Application	Mozilla	Firefox	3.6	All	All	All
Application	Mozilla	Firefox	3.6	a1_pre	All	All
Application	Mozilla	Firefox	3.6.1	All	All	All
Application	Mozilla	Firefox	3.7	a1_pre	All	All
Application	Mozilla	Firefox	3.7	alpha1	All	All
Application	Mozilla	Firefox	3.7	alpha2	All	All
Application	Mozilla	Firefox	3.6	All	All	All
Application	Mozilla	Firefox	3.6	a1_pre	All	All
Application	Mozilla	Firefox	3.6.1	All	All	All
Application	Mozilla	Firefox	3.7	a1_pre	All	All

Application	Mozilla	Firefox	3.7	alpha1	All	All
Application	Mozilla	Firefox	3.7	alpha2	All	All

cpe:2.3:o:microsoft:windows_vista:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6:a1_pre:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.7:a1_pre:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.7:alpha1:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.7:alpha2:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6:a1_pre:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.7:a1_pre:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.7:alpha1:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.7:alpha2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→