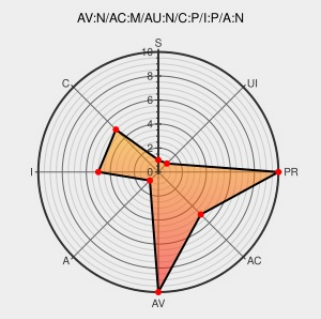
CVE-2010-3399

Published on: 09/15/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:02 PM UTC

CVE-2010-3399

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



Certain versions of Firefox from Mozilla contain the following vulnerability:

The js_InitRandom function in the JavaScript implementation in Mozilla Firefox 3.5.10 through 3.5.11, 3.6.4 through 3.6.8, and 4.0 Beta1 uses a context pointer in conjunction with its successor pointer for seeding of a random number generator, which makes it easier for remote attackers to guess the seed value via a brute-force attack, a different vulnerability than CVE-2010-3171.

CVE-2010-3399 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2011-0061
IBM Security Trusteer Fraud Protection Software | IBM	Exploit www.trusteer.com application/pdf	MISC www.trusteer.com/sites/default/files/Cross_domain_Math_Random_leakage_in_FF_3.6.4 3.6.8.pdf
Oracle Solaris Firefox Multiple Vulnerabilities - Advisories - Community	web.archive.org text/html	SECUNIA 42867

Community		
NEOHAPSIS - Peace of Mind Through Integrity and Insight	web.archive.org text/html Inactive Link Not Archived	BUGTRAQ 20100914 New writeup by Amit Klein (Trusteer): "Cross-domain information leakage in Firefox 3.6.4-3.6.8, Firefox 3.5.10-3.5.11 and Firefox 4.0 Beta1"
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:7598
475585 – (CVE-2008-5913) Re-seed Math.random() for each window/frame/context	bugzilla.mozilla.org text/html	MISC bugzilla.mozilla.org/show_bug.cgi?id=475585
577512 – (CVE-2010-3171) (more) cross-domain information leakage with Math.random()	bugzilla.mozilla.org text/html	MISC bugzilla.mozilla.org/show_bug.cgi?id=577512
Security	web.archive.org text/html Inactive Link Not Archived	CONFIRM blogs.sun.com/security/entry/multiple_vulnerabilities_in_mozilla_firefox

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	3.5.10	All	All	All
Application	Mozilla	Firefox	3.5.11	All	All	All
Application	Mozilla	Firefox	3.6.4	All	All	All
Application	Mozilla	Firefox	3.6.6	All	All	All
Application	Mozilla	Firefox	3.6.7	All	All	All
Application	Mozilla	Firefox	3.6.8	All	All	All
Application	Mozilla	Firefox	4.0	beta1	All	All
Application	Mozilla	Firefox	3.5.10	All	All	All
Application	Mozilla	Firefox	3.5.11	All	All	All
Application	Mozilla	Firefox	3.6.4	All	All	All
Application	Mozilla	Firefox	3.6.6	All	All	All
Application	Mozilla	Firefox	3.6.7	All	All	All
Application	Mozilla	Firefox	3.6.8	All	All	All
Application	Mozilla	Firefox	4.0	beta1	All	All

cpe:2.3:a:mozilla:firefox:3.5.10:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.5.11:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.6.4:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.6.6:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.6.7:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.6.8:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:4.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.5.10:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.5.11:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.6.4:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.6.6:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.6.7:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.6.8:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:4.0:beta1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→