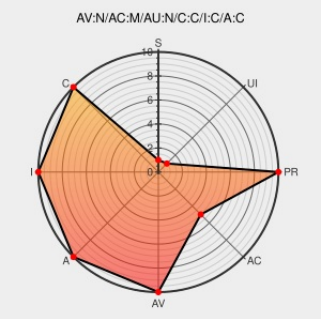
CVE-2009-3378

Published on: 10/29/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:25 PM UTC

CVE-2009-3378

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



Certain versions of Firefox from Mozilla contain the following vulnerability:

The oggplay_data_handle_theora_frame function in media/liboggplay/src/liboggplay/oggplay_data.c in liboggplay, as used in Mozilla Firefox 3.5.x before 3.5.4, attempts to reuse an earlier frame data structure upon encountering a decoding error for the first frame, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly execute arbitrary code via a crafted .ogg video file.

CVE-2009-3378 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
No Description Provided	sunsolve.sun.com Inactive Link Not Archived	SUNALERT 272909
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:6443
MFSA 2009-63: Upgrade media libraries to fix memory safety bugs	Patch Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/2009/mfsa2009-63.html

500311 – crash while loading video clip [@ memcpy - oggplay_data_handle_theora_frame]	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=500311
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2009-3334
Support / Security / Advisories / / MDVSA-2009:294 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2009:294

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	3.5.1	All	All	All
Application	Mozilla	Firefox	3.5.2	All	All	All
Application	Mozilla	Firefox	3.5.3	All	All	All
Application	Mozilla	Firefox	3.5.1	All	All	All
Application	Mozilla	Firefox	3.5.2	All	All	All
Application	Mozilla	Firefox	3.5.3	All	All	All

cpe:2.3:a:mozilla:firefox:3.5.1:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.5.2:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.5.3:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.5.1:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.5.2:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:3.5.3:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report