

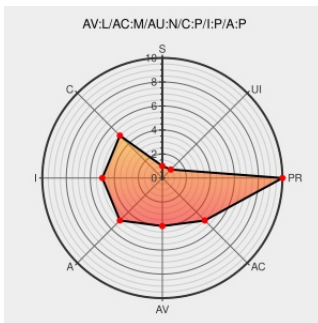


CVE-2009-3274

Published on: 09/21/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:24 PM UTC

CVE-2009-3274

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

Mozilla Firefox 3.6a1, 3.5.3, 3.5.2, and earlier 3.5.x versions, and 3.0.14 and earlier 2.x and 3.x versions, on Linux uses a predictable /tmp pathname for files selected from the Downloads window, which allows local users to replace an arbitrary downloaded file by placing a file in a /tmp location before the download occurs, related to the

Download Manager component. NOTE: some of these details are obtained from third party information.

CVE-2009-3274 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.4 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

No Description Provided

Broken Link

[sunsolve.sun.com](#)

[SUNALERT 272909](#)

Inactive Link Not Archived

Mozilla Firefox Temporary File Download Manipulation Security Issue - Secunia Advisories - Vulnerability Information - Secunia.com

Third Party Advisory

[web.archive.org](#)

text/html

[SECUNIA 36649](#)

Zero Day Demos (Firefox Vulnerability Discovered) Tutorial

[securitytube.net](#)

text/html

[MISC securitytube.net/Zero-Day-Demos-\(Firefox-Vulnerability-Discovered\)-video.aspx](#)

Webmail - OVH	Third Party Advisory www.vupen.com text/html	 VUPEN ADV-2010-0650
Support Red Hat	Third Party Advisory www.redhat.com text/html	 REDHAT RHSA-2010:0153
Support	Third Party Advisory www.redhat.com text/html	 REDHAT RHSA-2010:0154
MFSA 2009-53: Local downloaded file tampering	Vendor Advisory www.mozilla.org text/html	 CONFIRM www.mozilla.org/security/announce/2009/mfsa2009-53.html
514823 – (CVE-2009-3274) Incremental filename choosing scheme for duplicate filenames vulnerable (especially with the use of /tmp)	Issue Tracking Vendor Advisory bugzilla.mozilla.org text/html	 CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=514823
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	 VUPEN ADV-2009-3334
Support / Security / Advisories // MDVSA-2009:294 Mandriva	Broken Link www.mandriva.com text/html	 MANDRIVA MDVSA-2009:294
security	Broken Link jbrownsec.blogspot.com text/html Inactive Link Not Archived	 MISC jbrownsec.blogspot.com/2009/09/vamos-updates.html
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:9641

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
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Application	Mozilla	Firefox	2.0	All	All	All
Application	Mozilla	Firefox	2.0.0.1	All	All	All
Application	Mozilla	Firefox	2.0.0.10	All	All	All
Application	Mozilla	Firefox	2.0.0.11	All	All	All
Application	Mozilla	Firefox	2.0.0.12	All	All	All

Application	Mozilla	Firefox	2.0.0.13	All	All	All
Application	Mozilla	Firefox	2.0.0.14	All	All	All
Application	Mozilla	Firefox	2.0.0.15	All	All	All
Application	Mozilla	Firefox	2.0.0.16	All	All	All
Application	Mozilla	Firefox	2.0.0.17	All	All	All
Application	Mozilla	Firefox	2.0.0.18	All	All	All
Application	Mozilla	Firefox	2.0.0.19	All	All	All
Application	Mozilla	Firefox	2.0.0.2	All	All	All
Application	Mozilla	Firefox	2.0.0.20	All	All	All
Application	Mozilla	Firefox	2.0.0.3	All	All	All
Application	Mozilla	Firefox	2.0.0.4	All	All	All
Application	Mozilla	Firefox	2.0.0.5	All	All	All
Application	Mozilla	Firefox	2.0.0.6	All	All	All
Application	Mozilla	Firefox	2.0.0.7	All	All	All
Application	Mozilla	Firefox	2.0.0.8	All	All	All
Application	Mozilla	Firefox	2.0.0.9	All	All	All
Application	Mozilla	Firefox	3.0	All	All	All
Application	Mozilla	Firefox	3.0.1	All	All	All
Application	Mozilla	Firefox	3.0.10	All	All	All
Application	Mozilla	Firefox	3.0.11	All	All	All
Application	Mozilla	Firefox	3.0.12	All	All	All
Application	Mozilla	Firefox	3.0.13	All	All	All
Application	Mozilla	Firefox	3.0.14	All	All	All
Application	Mozilla	Firefox	3.0.2	All	All	All
Application	Mozilla	Firefox	3.0.3	All	All	All
Application	Mozilla	Firefox	3.0.4	All	All	All
Application	Mozilla	Firefox	3.0.5	All	All	All
Application	Mozilla	Firefox	3.0.6	All	All	All
Application	Mozilla	Firefox	3.0.7	All	All	All
Application	Mozilla	Firefox	3.0.8	All	All	All
Application	Mozilla	Firefox	3.0.9	All	All	All
Application	Mozilla	Firefox	3.5	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

Application	Mozilla	Firefox	3.6	a1	All	All
Application	Mozilla	Firefox	2.0	All	All	All
Application	Mozilla	Firefox	2.0.0.1	All	All	All
Application	Mozilla	Firefox	2.0.0.10	All	All	All
Application	Mozilla	Firefox	2.0.0.11	All	All	All
Application	Mozilla	Firefox	2.0.0.12	All	All	All
Application	Mozilla	Firefox	2.0.0.13	All	All	All
Application	Mozilla	Firefox	2.0.0.14	All	All	All
Application	Mozilla	Firefox	2.0.0.15	All	All	All
Application	Mozilla	Firefox	2.0.0.16	All	All	All
Application	Mozilla	Firefox	2.0.0.17	All	All	All
Application	Mozilla	Firefox	2.0.0.18	All	All	All
Application	Mozilla	Firefox	2.0.0.19	All	All	All
Application	Mozilla	Firefox	2.0.0.2	All	All	All
Application	Mozilla	Firefox	2.0.0.20	All	All	All
Application	Mozilla	Firefox	2.0.0.3	All	All	All
Application	Mozilla	Firefox	2.0.0.4	All	All	All
Application	Mozilla	Firefox	2.0.0.5	All	All	All
Application	Mozilla	Firefox	2.0.0.6	All	All	All
Application	Mozilla	Firefox	2.0.0.7	All	All	All
Application	Mozilla	Firefox	2.0.0.8	All	All	All
Application	Mozilla	Firefox	2.0.0.9	All	All	All
Application	Mozilla	Firefox	3.0	All	All	All
Application	Mozilla	Firefox	3.0.1	All	All	All
Application	Mozilla	Firefox	3.0.10	All	All	All
Application	Mozilla	Firefox	3.0.11	All	All	All
Application	Mozilla	Firefox	3.0.12	All	All	All
Application	Mozilla	Firefox	3.0.13	All	All	All
Application	Mozilla	Firefox	3.0.14	All	All	All
Application	Mozilla	Firefox	3.0.2	All	All	All
Application	Mozilla	Firefox	3.0.3	All	All	All
Application	Mozilla	Firefox	3.0.4	All	All	All
Application	Mozilla	Firefox	3.0.5	All	All	All
Application	Mozilla	Firefox	3.0.6	All	All	All
Application	Mozilla	Firefox	3.0.7	All	All	All
Application	Mozilla	Firefox	3.0.8	All	All	All

Application	Mozilla	Firefox	3.0.9	All	All	All
Application	Mozilla	Firefox	3.5	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
Application	Mozilla	Firefox	3.6	a1	All	All
cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.1:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.10:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.11:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.12:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.13:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.14:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.15:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.16:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.17:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.18:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.19:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.2:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.20:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.3:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.4:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.5:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.6:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.7:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.8:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:2.0.0.9:*:*:*:*:*:						

cpe:2.3:a:mozilla:firefox:3.0:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.1:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.10:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.11:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.12:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.13:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.14:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.2:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.3:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.4:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.5:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.6:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.7:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.8:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.0.9:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:3.5:*:*:*:*:*:
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:3.6:a1:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:2.0:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:2.0.0.1:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:2.0.0.10:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:2.0.0.11:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:2.0.0.12:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:2.0.0.13:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:2.0.0.14:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:2.0.0.15:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:2.0.0.16:*:*:*:*:*:

```
cpe:2.3:a:mozilla:firefox:2.0.0.17:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:2.0.0.18:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:2.0.0.19:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:2.0.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:2.0.0.20:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:2.0.0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:2.0.0.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:2.0.0.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:2.0.0.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:2.0.0.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:2.0.0.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:2.0.0.9:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.10:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.11:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.12:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.13:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.14:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.0.9:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox:3.5:*:*:*:*:*:*:
```

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:3.6:a1:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)