

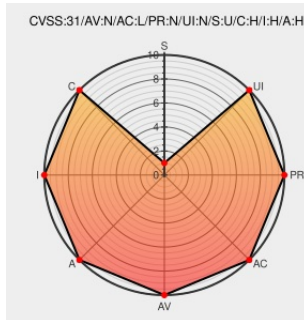


CVE-2013-5616

Published on: 12/11/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:36 PM UTC

CVE-2013-5616

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

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

Use-after-free vulnerability in the nsEventListenerManager::HandleEventSubType function in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors related to mListeners event listeners.

CVE-2013-5616 has been assigned by [m](#) security@mozilla.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Oracle Solaris Bulletin - April 2016	Third Party Advisory www.oracle.com	CONFIRM www.oracle.com/technetwork/topics/security/bulletinapr2016-

	text/html	2952098.html
openSUSE-SU-2014:0008-1: moderate: update for seamonkey	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2014:0008
openSUSE-SU-2013:1958-1: moderate: update for MozillaThunderbird	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1958
USN-2052-1: Firefox vulnerabilities Ubuntu	Third Party Advisory www.ubuntu.com text/html	 UBUNTU USN-2052-1
[SECURITY] Fedora 20 Update: firefox-26.0-3.fc20	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2013-23519
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code and Conduct Cross-Site Scripting Attacks - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTrack 1029470
[SECURITY] Fedora 18 Update: thunderbird-24.2.0-2.fc18	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2013-23291
[security-announce] SUSE-SU-2013:1919-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SU-2013:1919
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2013:1812
Gentoo Security	Third Party Advisory security.gentoo.org text/html	 GENTOO GLSA-201504-01
Mozilla Seamonkey Multiple Flaws Let Remote Users Execute Arbitrary Code and Conduct Cross-Site Scripting Attacks - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTrack 1029476
openSUSE-SU-2013:1918-1: moderate: update for MozillaFirefox	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1918
USN-2053-1: Thunderbird vulnerabilities Ubuntu	Third Party Advisory www.ubuntu.com text/html	 UBUNTU USN-2053-1
[SECURITY] Fedora 19 Update: firefox-26.0-2.fc19	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2013-23127
openSUSE-SU-2013:1917-1: moderate: update for MozillaFirefox	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1917

	text/html	
openSUSE-SU-2013:1916-1: moderate: update for MozillaFirefox	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1916
openSUSE-SU-2013:1957-1: moderate: update for MozillaThunderbird	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1957
Access Denied	Exploit Issue Tracking Vendor Advisory bugzilla.mozilla.org text/html	 CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=938341
MFSA 2013-108: Use-after-free in event listeners	Vendor Advisory www.mozilla.org text/html	 CONFIRM www.mozilla.org/security/announce/2013/mfsa2013-108.html
[SECURITY] Fedora 19 Update: thunderbird-24.2.0-2.fc19	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2013-23295
openSUSE-SU-2013:1959-1: moderate: update for MozillaThunderbird	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1959

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	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All

Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Fedoraproject	Fedora	18	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	18	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.5	All	All	All

Operating System	Redhat	Enterprise Linux Eus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All
Application	Suse	Suse Linux Enterprise Software Development Kit	11.0	sp3	All	All
Application	Suse	Suse Linux Enterprise Software Development Kit	11.0	sp3	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:						

```
cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:canonical:ubuntu_linux:13.04:*:*:*:*:*:*:
```

```
cpe:2.3:o:canonical:ubuntu_linux:13.10:*:*:*:*:*:*:
```

```
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*
```

```
cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:
```

```
cpe:2.3:o:canonical:ubuntu_linux:13.04:*:*:*:*:*:*:
```

```
cpe:2.3:o:canonical:ubuntu_linux:13.10:*:*:*:*:*:*:
```

```
cpe:2.3:o:fedoraproject:fedora:18:*:*:*:*:*:
```

```
cpe:2.3:o:fedoraproject:fedora:19:*:*:*:*:*:
```

```
cpe:2.3:o:fedoraproject:fedora:20:*:*:*:*:*:*:
```

```
cpe:2.3:o:fedoraproject:fedora:18:*:*:*:*:*:
```

```
cpe:2.3:o:fedoraproject:fedora:19:*:*:*:*:*:*:
```

```
cpe:2.3:o:fedoraproject:fedora:20:*:*:*:*:*:
```

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

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

```
cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:*.:.:.:.:.:.:
```

```
cpe:2.3:a:mozilla:seamonkey:*.:.:.:.:.:.:
```

```
cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:12.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:12.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop:5.0:*:*:*:*:*:*
```

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:5.0:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:6.5:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:6.5:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:5.0:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:5.0:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:6.5:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:6.5:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:6.5:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:6.5:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:6.5:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:6.5:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:5.0:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:5.0:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_desktop:11:sp3:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_desktop:11:sp3:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp3:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp3:*:*:*:vmware:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp3:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp3:*:*:*:vmware:*:*:

cpe:2.3:a:suse:suse_linux_enterprise_software_development_kit:11.0:sp3:*:*:*:*:*:

cpe:2.3:a:suse:suse_linux_enterprise_software_development_kit:11.0:sp3:*:*:*:*:*:

No vendor comments have been submitted for this CVE

© [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](#)