



# CVE-2015-8837

Published on: 03/30/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

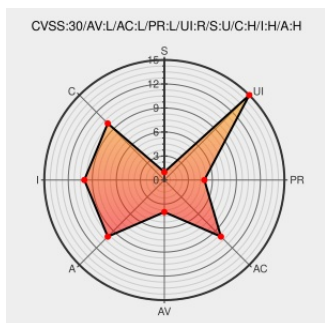
## CVE-2015-8837

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Stack-based buffer overflow in the `isofs_real_readdir` function in `isofs.c` in `FuseISO 20070708` allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long pathname in an ISO file.

CVE-2015-8837 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.3 - HIGH**

| Attack Vector | Attack Complexity      | Privileges Required | User Interaction    |
|---------------|------------------------|---------------------|---------------------|
| LOCAL         | LOW                    | LOW                 | REQUIRED            |
| Scope         | Confidentiality Impact | Integrity Impact    | Availability Impact |
| UNCHANGED     | HIGH                   | HIGH                | HIGH                |

CVSS2 Score: **6.8 - MEDIUM**

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

## CVE References

| Description                                                                          | Tags                                                                                                                                                   | Link                                                                                  |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Bug 862211 – fuseiso: stack-based buffer overflow in <code>isofs_real_readdir</code> | <a href="#">Exploit</a><br><a href="#">Issue Tracking</a><br><a href="#">Patch</a><br><a href="#">bugzilla.redhat.com</a><br><a href="#">text/html</a> | <a href="#">CONFIRM</a><br><a href="#">bugzilla.redhat.com/show_bug.cgi?id=862211</a> |

|                                                                                                                             |                                                                                                                                                            |                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| oss-security - Re: older fuseiso stuff                                                                                      | <a href="http://www.openwall.com">www.openwall.com</a><br><a href="#">text/html</a>                                                                        |  <a href="#">MLIST [oss-security] 20150223</a><br>Re: older fuseiso stuff                                                              |
| Bug 863091 – CVE-2015-8837 fuseiso: Stack-based buffer overflow when scanning directory structure for absolute path entries | <a href="#">Issue Tracking</a><br><a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a><br><a href="#">text/html</a>                                |  <a href="#">CONFIRM</a><br><a href="http://bugzilla.redhat.com/show_bug.cgi?id=863091">bugzilla.redhat.com/show_bug.cgi?id=863091</a> |
| Debian -- Security Information -- DSA-3551-1 fuseiso                                                                        | <a href="#">Third Party Advisory</a><br><a href="http://www.debian.org">www.debian.org</a><br><a href="#">Deprecated Link</a><br><a href="#">text/html</a> |  <a href="#">DEBIAN DSA-3551</a>                                                                                                       |
| oss-security - older fuseiso stuff                                                                                          | <a href="http://www.openwall.com">www.openwall.com</a><br><a href="#">text/html</a>                                                                        |  <a href="#">MLIST [oss-security] 20150206</a><br>older fuseiso stuff                                                                  |
| fuseiso: Multiple vulnerabilities (GLSA 202007-20) — Gentoo security                                                        | <a href="http://security.gentoo.org">security.gentoo.org</a><br><a href="#">text/html</a>                                                                  |  <a href="#">GENTOO GLSA-202007-20</a>                                                                                                 |

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](mailto:comment@cve.report).

## Related QID Numbers

671413 EulerOS Security Update for fuseiso (EulerOS-SA-2022-1319)

671665 EulerOS Security Update for fuseiso (EulerOS-SA-2022-1719)

## Known Affected Configurations (CPE V2.3)

| Type                                         | Vendor          | Product      | Version | Update | Edition | Language |
|----------------------------------------------|-----------------|--------------|---------|--------|---------|----------|
| Operating System                             | Debian          | Debian Linux | 7.0     | All    | All     | All      |
| Operating System                             | Debian          | Debian Linux | 8.0     | All    | All     | All      |
| Operating System                             | Debian          | Debian Linux | 7.0     | All    | All     | All      |
| Operating System                             | Debian          | Debian Linux | 8.0     | All    | All     | All      |
| Operating System                             | Fedoraproject   | Fedora       | 16      | All    | All     | All      |
| Operating System                             | Fedoraproject   | Fedora       | 17      | All    | All     | All      |
| Operating System                             | Fedoraproject   | Fedora       | 16      | All    | All     | All      |
| Operating System                             | Fedoraproject   | Fedora       | 17      | All    | All     | All      |
| Application                                  | Fuseiso Project | Fuseiso      | All     | All    | All     | All      |
| cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*: |                 |              |         |        |         |          |
| cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*: |                 |              |         |        |         |          |

|                                          |
|------------------------------------------|
| cpe:2.3:o:debian:debian_linux:7.0:*****: |
| cpe:2.3:o:debian:debian_linux:8.0:*****: |
| cpe:2.3:o:fedoraproject:fedora:16:*****: |
| cpe:2.3:o:fedoraproject:fedora:17:*****: |
| cpe:2.3:o:fedoraproject:fedora:16:*****: |
| cpe:2.3:o:fedoraproject:fedora:17:*****: |
| cpe:2.3:a:fuseiso_project:fuseiso:*****: |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)