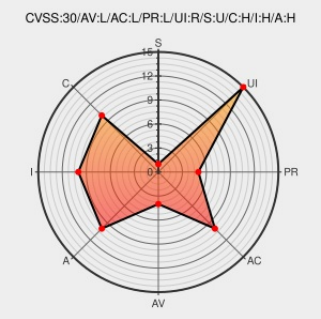
CVE-2015-8836

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

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

CVE-2015-8836

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

Integer overflow in the isofs_real_read_zf function in isofs.c in FuseISO 20070708 might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a large ZF block size in an ISO file, leading to a heap-based buffer overflow.

CVE-2015-8836 has been assigned by 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
oss-security - Re: older fuseiso stuff	Mailing List, www.openwall.com, text/html	MLIST [oss-security] 20150223 Re: older fuseiso stuff

Bug 863102 – CVE-2015-8836 fuseiso: Integer overflow, leading to heap buffer overflow when reading certain ISO ZF blocks	Issue Tracking bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=863102
Debian -- Security Information -- DSA-3551-1 fuseiso	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3551
Bug 861358 – fuseiso: integer overflow in isofs_real_read_zf	Exploit Issue Tracking Patch Technical Description bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=861358
oss-security - older fuseiso stuff	Mailing List www.openwall.com text/html	MLIST [oss-security] 20150206 older fuseiso stuff

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.

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	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: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→

© 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 registred 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