

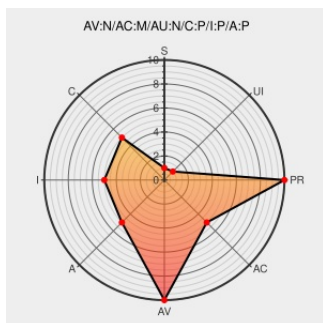


CVE-2013-5648

Published on: 08/29/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:37 PM UTC

CVE-2013-5648

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

Certain versions of [ld-software](#) from [ld](#) contain the following vulnerability:

Absolute path traversal vulnerability in the handleStartDataFile function in DigiDocSAXParser.c in libdigidoc 3.6.0.0, as used in ID-software before 3.7.2 and other products, allows remote attackers to overwrite arbitrary files via a filename beginning with / (slash) or \ (backslash) in a DDOC file.

CVE-2013-5648 has been assigned by [M](#) cve@mitre.org to track the vulnerability

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

1002299 – (CVE-2013-5648) CVE-2013-5648
libdigidoc: arbitrary file overwrite flaw

[bugzilla.redhat.com](#)
[text/html](#)

[CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1002299](#)

[packages] Contents of
/updates/3/libdigidoc/current/SOURCES/libdigidoc-
3.6.0.0-security-fix-DataFile-name-tag.patch

[Patch](#)
[svnweb.mageia.org](#)
[text/html](#)

[CONFIRM](#)
[svnweb.mageia.org/packages/updates/3/libdigidoc/current/SOURC
3.6.0.0-security-fix-DataFile-name-tag.patch?revision=472660&view](#)

11100 – libdigidoc new security issue CVE-2013-
5648

[bugs.mageia.org](#)
[text/html](#)

[CONFIRM bugs.mageia.org/show_bug.cgi?id=11100](#)

ID-software version information (release notes)
> Release notes > ID-software instructions and
problem solutions > HELP CENTRE > ID.ee

[www.id.ee](#)
[text/html](#)

[CONFIRM www.id.ee/?lang=en&id=34283#3_7_2](#)

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	Id	Id-software	3.7	All	All	All
Application	Id	Id-software	3.7.1	All	All	All
Application	Id	Id-software	3.7	All	All	All
Application	Id	Id-software	3.7.1	All	All	All
Application	Id	Libdigidoc	3.6.0.0	All	All	All
Application	Id	Libdigidoc	3.6.0.0	All	All	All
cpe:2.3:a:id:id-software:3.7:*:*:*:*:*:						
cpe:2.3:a:id:id-software:3.7.1:*:*:*:*:*:						
cpe:2.3:a:id:id-software:3.7:*:*:*:*:*:						
cpe:2.3:a:id:id-software:3.7.1:*:*:*:*:*:						
cpe:2.3:a:id:libdigidoc:3.6.0.0:*:*:*:*:*:						
cpe:2.3:a:id:libdigidoc:3.6.0.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→