



CVE-2015-7358

Published on: 10/02/2017 12:00:00 AM UTC

Last Modified on: 06/28/2021 06:20:00 PM UTC

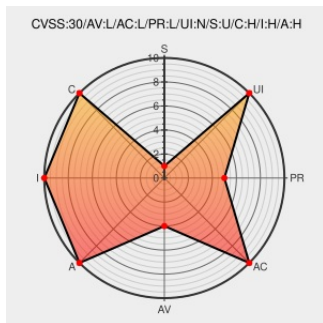
CVE-2015-7358

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 



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

The `IsDriveLetterAvailable` method in `Driver/Ntdriver.c` in TrueCrypt 7.0, VeraCrypt before 1.15, and CipherShed, when running on Windows, does not properly validate drive letter symbolic links, which allows local users to mount an encrypted volume over an existing drive letter and gain privileges via an entry in the `/GLOBAL??` directory.

CVE-2015-7358 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
oss-security - CVE Request - TrueCrypt 7.1a and VeraCrypt 1.14 Local Elevation of Privilege	Mailing List Third Party Advisory www.openwall.com	MLIST [oss-security] 20150922 CVE Request - TrueCrypt 7.1a and VeraCrypt 1.14 Local Elevation of Privilege

Issue 538 - google-security-research - Truecrypt 7 Derived Code/Windows: Drive Letter Symbolic Link Creation EoP - Google Security Research - Google Project Hosting	text/html Third Party Advisory code.google.com text/html	🌐 MISC code.google.com/p/google-security-research/issues/detail?id=538
oss-security - Re: CVE Request - TrueCrypt 7.1a and VeraCrypt 1.14 Local Elevation of Privilege	Issue Tracking Mailing List Third Party Advisory www.openwall.com text/html	🔗 MLIST [oss-security] 20150924 Re: CVE Request - TrueCrypt 7.1a and VeraCrypt 1.14 Local Elevation of Privilege
Truecrypt 7 Derived Code/Windows: Drive Letter Symbolic Link Creation Privilege Escalation ~ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	📄 MISC packetstormsecurity.com/files/133878/Truecrypt-7-Derived-Code-Windows-Drive-Letter-Symbolic-Link-Creation-Privilege-Escalation.html
VeraCrypt - Documentation	Release Notes Vendor Advisory veracrypt.codeplex.com text/html	🌐 CONFIRM veracrypt.codeplex.com/wikipage?title=Release%20Notes
TrueCrypt 7 / VeraCrypt 1.13 - Drive Letter Symbolic Link Creation Privilege Escalation	Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	🔥 EXPLOIT-DB 38403

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	Ciphershed	Ciphershed	All	All	All	All
Application	Idrix	Veracrypt	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Application	Truecrypt	Truecrypt	7.0	All	All	All
Application	Truecrypt	Truecrypt	7.0	All	All	All
Application	Veracrypt	Veracrypt	All	All	All	All
cpe:2.3:a:ciphershed:ciphershed:*****:						
cpe:2.3:a:idrix:veracrypt:*****:						
cpe:2.3:o:microsoft:windows:*****:						
cpe:2.3:o:microsoft:windows:*****:						

cpe:2.3:a:truecrypt:truecrypt:7.0:*:*:*:*:*:

cpe:2.3:a:truecrypt:truecrypt:7.0:*:*:*:*:*:

cpe:2.3:a:veracrypt:veracrypt:*:*:*:*:*:

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](#)