



CVE-2019-13313

Published on: 07/05/2019 12:00:00 AM UTC

Last Modified on: 02/28/2023 08:49:00 PM UTC

CVE-2019-13313

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

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

libosinfo 1.5.0 allows local users to discover credentials by listing a process, because credentials are passed to osinfo-install-script via the command line.

CVE-2019-13313 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: **2.1 - LOW**

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

CVE References

Description	Tags	Link
[Libosinfo] [libosinfo PATCH 0/2] Do not expose user & admin password in	Mailing List Patch Third Party Advisory www.redhat.com text/html	MISC www.redhat.com/archives/libosinfo/2019-July/msg00026.html

[SECURITY] Fedora 29 Update: libosinfo-1.2.0-8.fc29 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-d2cde4761e
libosinfo Download official releases	Release Notes Vendor Advisory libosinfo.org text/html	 MISC libosinfo.org/download/
Tags · libosinfo / libosinfo · GitLab	Release Notes Third Party Advisory gitlab.com text/html	 MISC gitlab.com/libosinfo/libosinfo/-/tags
[SECURITY] Fedora 30 Update: mingw-libosinfo-1.4.0-3.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-e23aeac13e
oss-security - CVE-2019-13313, CVE-2019-13314: password disclosure via command line arguments	Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20190708 CVE-2019-13313, CVE-2019-13314: password disclosure via command line arguments
[SECURITY] Fedora 29 Update: mingw-libosinfo-1.2.0-2.fc29 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-4b8990e4d6
NEWS · master · libosinfo / libosinfo · GitLab	Release Notes Third Party Advisory gitlab.com text/html	 MISC gitlab.com/libosinfo/libosinfo/blob/master/NEWS
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:3387
[SECURITY] Fedora 30 Update: libosinfo-1.4.0-4.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-c9fbe3db9c

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

[377352](#) Alibaba Cloud Linux Security Update for osinfo-db and libosinfo (ALINUX3-SA-2022:0044)

[377469](#) Alibaba Cloud Linux Security Update for libosinfo (ALINUX2-SA-2020:0053)

[501045](#) Alpine Linux Security Update for libosinfo

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Application	Libosinfo	Libosinfo	1.5.0	All	All	All
Application	Libosinfo	Libosinfo	1.5.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

Operating System	Redhat	Enterprise Linux Eus	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.6	All	All	All
cpe:2.3:o:fedoraproject:fedora:29:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:						
cpe:2.3:a:libosinfo:libosinfo:1.5.0:*:*:*:*:*:						
cpe:2.3:a:libosinfo:libosinfo:1.5.0:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_eus:8.1:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_eus:8.2:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_eus:8.4:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_eus:8.6:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_server_aus:8.2:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_server_aus:8.4:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_server_aus:8.6:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_server_tus:8.2:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_server_tus:8.4:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_server_tus:8.6:*:*:*:*:*:						

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](#)