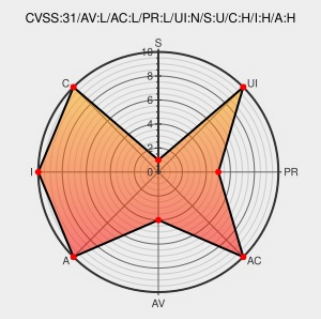
# CVE-2019-3500

Published on: 01/02/2019 12:00:00 AM UTC

Last Modified on: 04/06/2022 06:33:00 PM UTC

## CVE-2019-3500

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




Certain versions of Aria2 from Aria2 Project contain the following vulnerability:

aria2c in aria2 1.33.1, when --log is used, can store an HTTP Basic Authentication username and password in a file, which might allow local users to obtain sensitive information by reading this file.

CVE-2019-3500 has been assigned by 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 |
|---|---|---|
| Metadata and potential password leaks via --log= · Issue #1329 · aria2/aria2 · GitHub | Patch, Third Party Advisory, github.com, text/html | MISC github.com/aria2/aria2/issues/1329 |

| | | |
|---|---|---|
| USN-3965-1: aria2 vulnerability \| Ubuntu security notices | usn.ubuntu.com<br>text/html | UBUNTU USN-3965-1 |
| [SECURITY] Fedora 28 Update: aria2-1.34.0-4.fc28 - package-announce - Fedora Mailing-Lists | Mailing List<br>Release Notes<br>Third Party Advisory<br>lists.fedoraproject.org<br>text/html | FEDORA FEDORA-2019-8b8c774b84 |
| [SECURITY] Fedora 30 Update: aria2-1.34.0-4.fc30 - package-announce - Fedora Mailing-Lists | Mailing List<br>Release Notes<br>Third Party Advisory<br>lists.fedoraproject.org<br>text/html | FEDORA FEDORA-2019-248ad990b4 |
| [SECURITY] [DLA 1636-1] aria2 security update | Mailing List<br>Third Party Advisory<br>lists.debian.org<br>text/html | MLIST [debian-lts-announce] 20190122 [SECURITY] [DLA 1636-1] aria2 security update |
| [SECURITY] [DLA 2873-1] aria2 security update | lists.debian.org<br>text/html | MLIST [debian-lts-announce] 20211230 [SECURITY] [DLA 2873-1] aria2 security update |
| [SECURITY] Fedora 29 Update: aria2-1.34.0-4.fc29 - package-announce - Fedora Mailing-Lists | Mailing List<br>Release Notes<br>Third Party Advisory<br>lists.fedoraproject.org<br>text/html | FEDORA FEDORA-2019-fa61af95b3 |

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

178980 Debian Security Update for aria2 (DLA 2873-1)

750954 OpenSUSE Security Update for aria2 (openSUSE-SU-2021:1125-1)

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Aria2 Project | Aria2 | 1.33.1 | All | All | All |
| Application | Aria2 Project | Aria2 | 1.33.1 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 19.04 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating | Fedoraproject | Fedora | 28 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| System | | | | | | |
| Operating System | Fedoraproject | Fedora | 29 | All | All | All |
| Operating System | Fedoraproject | Fedora | 30 | All | All | All |
| Operating System | Fedoraproject | Fedora | 28 | All | All | All |
| Operating System | Fedoraproject | Fedora | 29 | All | All | All |
| Operating System | Fedoraproject | Fedora | 30 | All | All | All |

cpe:2.3:a:aria2_project:aria2:1.33.1:*:*:*:*:*:*:*:

cpe:2.3:a:aria2_project:aria2:1.33.1:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:28:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:29:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:28:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:29:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|

← 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**