



# CVE-2019-5094

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-5094
<b>State</b>	PUBLIC
<b>Assigner</b>	talos-cna@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-09-24 22:15:00 UTC
<b>Updated</b>	2023-11-07 03:11:00 UTC
<b>Description</b>	An exploitable code execution vulnerability exists in the quota file functionality of E2fsprogs 1.45.3. A specially crafted ext4

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">E2fsprogs Project</a>	<a href="#">E2fsprogs</a>	All	All	All	All

Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 30 Update: e2fsprogs-1.44.6-2.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] [DLA 1935-1] e2fsprogs security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[SECURITY] Fedora 31 Update: e2fsprogs-1.45.5-1.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 31 Update: e2fsprogs-1.45.5-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: e2fsprogs-1.44.6-2.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
e2fsprogs: Arbitrary code execution (GLSA 202003-05) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
CVE-2019-5094 E2FSProgs Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
TALOS-2019-0887    Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	<a href="https://talosintelligence.com">talosintelligence.com</a>
USN-4142-2: e2fsprogs vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
Bugtraq: [SECURITY] [DSA 4535-1] e2fsprogs security update	BUGTRAQ	<a href="https://seclists.org">seclists.org</a>
USN-4142-1: e2fsprogs vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
Debian -- Security Information -- DSA-4535-1 e2fsprogs	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[375305](#) EulerOS Security Update for e2fsprogs (EulerOS-SA-2021-1290)

[377536](#) Alibaba Cloud Linux Security Update for e2fsprogs (ALINUX2-SA-2020:0152)

[500170](#) Alpine Linux Security Update for e2fsprogs

[503905](#) Alpine Linux Security Update for e2fsprogs

[591406](#) Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

[670299](#) EulerOS Security Update for e2fsprogs (EulerOS-SA-2021-1777)

[671127](#) EulerOS Security Update for e2fsprogs (EulerOS-SA-2019-2140)

[900188](#) CBL-Mariner Linux Security Update for e2fsprogs 1.44.6

[903592](#) Common Base Linux Mariner (CBL-Mariner) Security Update for e2fsprogs (3724)

© [CVE.report](#) 2026 |

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](#)