CVE-2022-1304

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-1304
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-14 21:15:00 UTC
Updated	2023-11-07 03:41:00 UTC
Description	An out-of-bounds read/write vulnerability was found in e2fsprogs 1.46.5. This issue leads to a segmentation fault and possil

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	E2fsprogs Project	E2fsprogs	1.46.5	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
2069726 – (CVE-2022-1304) CVE-2022-1304 e2fsprogs: out-of-bounds read/write via crafted filesystem	MISC	bugzilla.redhat.com
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160243 Oracle Enterprise Linux Security Update for e2fsprogs (ELSA-2022-7720)

160283 Oracle Enterprise Linux Security Update for e2fsprogs (ELSA-2022-8361)

183162 Debian Security Update for e2fsprogs (CVE-2022-1304)

198819 Ubuntu Security Notification for E2fsprogs Vulnerability (USN-5464-1)

240840 Red Hat Update for e2fsprogs (RHSA-2022:7720)

240917 Red Hat Update for e2fsprogs (RHSA-2022:8361)

354124 Amazon Linux Security Advisory for e2fsprogs : ALAS2-2022-1884

354380 Amazon Linux Security Advisory for e2fsprogs : ALAS2022-2022-228

354578 Amazon Linux Security Advisory for e2fsprogs : ALAS-2022-228

355133 Amazon Linux Security Advisory for e2fsprogs : ALAS2023-2023-044

502674 Alpine Linux Security Update for e2fsprogs

502980 Alpine Linux Security Update for e2fsprogs

503907 Alpine Linux Security Update for e2fsprogs

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

6140087 AWS Bottlerocket Security Update for e2fsprogs (GHSA-qh9x-999x-wqhr)

671861 EulerOS Security Update for e2fsprogs (EulerOS-SA-2022-1887)

672242 EulerOS Security Update for e2fsprogs (EulerOS-SA-2022-2600)

672268 EulerOS Security Update for e2fsprogs (EulerOS-SA-2022-2647)

672280 EulerOS Security Update for e2fsprogs (EulerOS-SA-2022-2679)

672706 EulerOS Security Update for e2fsprogs (EulerOS-SA-2023-1439)

672732 EulerOS Security Update for e2fsprogs (EulerOS-SA-2023-1464)

672878 EulerOS Security Update for e2fsprogs (EulerOS-SA-2023-1592)

690875 Free Berkeley Software Distribution (FreeBSD) Security Update for e2fsprogs (a58f3fde-e4e0-11ec-8340-2d623369b8b5)

710868 Gentoo Linux e2fsprogs Arbitrary Code Execution Vulnerability (GLSA 202402-15)

752122 SUSE Enterprise Linux Security Update for e2fsprogs (SUSE-SU-2022:1652-1)

752128 SUSE Enterprise Linux Security Update for e2fsprogs (SUSE-SU-2022:1688-1)

752139 SUSE Enterprise Linux Security Update for e2fsprogs (SUSE-SU-2022:1695-1)

752141 SUSE Enterprise Linux Security Update for e2fsprogs (SUSE-SU-2022:1718-1)

901636 Common Base Linux Mariner (CBL-Mariner) Security Update for e2fsprogs (9407)

903896 Common Base Linux Mariner (CBL-Mariner) Security Update for e2fsprogs (9407-1)

940735 AlmaLinux Security Update for e2fsprogs (ALSA-2022:7720)

940788 AlmaLinux Security Update for e2fsprogs (ALSA-2022:8361)

960296 Rocky Linux Security Update for e2fsprogs (RLSA-2022:7720)

960592 Rocky Linux Security Update for e2fsprogs (RLSA-2022:8361)

© 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 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