



CVE-2022-4055

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-4055
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-19 00:15:00 UTC
Updated	2022-11-26 03:18:00 UTC
Description	When xdg-mail is configured to use thunderbird for mailto URLs, improper parsing of the URL can lead to additional header

Risk And Classification

Problem Types: CWE-146

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freedesktop	Xdg-utils	All	All	All	All

References

Reference	Source	Link	T
xdg-email does not parse mailto uris properly for thunderbird (#205) · Issues · xdg / xdg-utils · GitLab	MISC	gitlab.freedesktop.org	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [354830](#) Amazon Linux Security Advisory for xdg-utils : ALAS2-2023-2002
- [355151](#) Amazon Linux Security Advisory for xdg-utils : ALAS2023-2023-007
- [904556](#) Common Base Linux Mariner (CBL-Mariner) Security Update for xdg-utils (11465)

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](#)