



CVE-2023-24069

Published on: Not Yet Published

Last Modified on: 01/26/2023 09:15:32 PM UTC

CVE-2023-24069

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

The following vulnerability was found:

**** DISPUTED **** Signal Desktop before 6.2.0 on Windows, Linux, and macOS allows an attacker to obtain potentially sensitive attachments sent in messages from the attachments.noindex directory. Cached attachments are not effectively cleared. In some cases, even after a self-initiated file deletion, an attacker can still recover the file if it was previously replied to in a conversation. (Local filesystem access is needed by the attacker.)
NOTE: the vendor disputes the relevance of this finding because the product is not intended to protect against adversaries with this degree of local access.

CVE-2023-24069 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVE References

Description	Tags	Link
Signal >> Download Signal for Windows	signal.org text/html	MISC signal.org/en/download/windows
John J Hacking	johnjhacking.com text/html	MISC johnjhacking.com/blog/cve-2023-24068-cve-2023-24069/
Signal >> Download Signal for Mac	signal.org text/html	MISC signal.org/download/macos
Signal >> Download Signal for Linux	signal.org text/html	MISC signal.org/download/linux









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.

There are currently no QIDs associated with this CVE

There are no known software configurations (CPEs) currently associated with this CVE

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @johnjhacking	Enjoy. Rather than read manic threads thrown all over the place, I've organized it for you - neatly :) johnjhacking.com/blog/cve-2023-... #infosec	2023-01-23 06:07:35
 @CVEreport	CVE-2023-24069 : Signal Desktop before 6.2.0 on #Windows, #Linux, and macOS allows an attacker to obtain potentiall... twitter.com/i/web/status/1...	2023-01-23 07:06:00
 @bytecodevm	CVE-2023-24068 && CVE-2023-24069: Abusing Signal Desktop Client for fun and for Espionage #research #messenger... twitter.com/i/web/status/1...	2023-01-23 11:13:31
 /r/signal	CVE-2023-24068 && CVE-2023-24069: Abusing Signal Desktop Client for fun and for Espionage	2023-01-24 14:40:53
 /r/InfoSecWriteups	Signal Client v6.2 and earlier versions vulnerable to CVE-2023-24068 & CVE-2023-24069	2023-01-24 07:51:28
 /r/privacy	CVE-2023-24068 && CVE-2023-24069: Abusing Signal Desktop Client for fun and for Espionage	2023-01-24 07:38:50
 /r/cybersecurity	CVE-2023-24068 && CVE-2023-24069: Abusing Signal Desktop Client for fun and for Espionage	2023-01-24 07:37:46
 /r/CKsTechNews	CVE-2023-24068 && CVE-2023-24069: Abusing Signal Desktop Client for fun and for Espionage	2023-01-24 19:37:59

[← 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