



CVE-2021-43844

Published on: Not Yet Published

Last Modified on: 01/04/2022 05:15:00 PM UTC

CVE-2021-43844 - advisory for GHSA-95v4-748v-fmf9

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Msedgeredirect](#) from [Msedgeredirect Project](#) contain the following vulnerability:

MSEdgeRedirect is a tool to redirect news, search, widgets, weather, and more to a user's default browser. MSEdgeRedirect versions before 0.5.0.1 are vulnerable to Remote Code Execution via specifically crafted URLs. This vulnerability requires user interaction and the acceptance of a prompt. With how MSEdgeRedirect is coded,

parameters are impossible to pass to any launched file. However, there are two possible scenarios in which an attacker can do more than a minor annoyance. In Scenario 1 (confirmed), a user visits an attacker controlled webpage; the user is prompted with, and downloads, an executable payload; the user is prompted with, and accepts, the aforementioned crafted URL prompt; and RCE executes the payload the user previously downloaded, if the download path is successfully guessed. In Scenario 2 (not yet confirmed), a user visits an attacked controlled webpage; the user is prompted with, and accepts, the aforementioned crafted URL prompt; and a payload on a remote, attacker controlled, SMB server is executed. The issue was found in the `_DecodeAndRun()` function, in which I incorrectly assumed `_WinAPI_Urlls()` would only accept web resources. Unfortunately, `file:///` passes the default `_WinAPI_Urlls` check(). File paths are now directly checked for and must fail. There is no currently known exploitation of this vulnerability in the wild. A patched version, 0.5.0.1, has been released that checks for and denies these crafted URLs. There are no workarounds for this issue. Users are advised not to accept any unexpected prompts from web pages.

CVE-2021-43844 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: rcmaehl - MSEdgeRedirect version < 0.5.0.1

CVSS3 Score: **8.8 - HIGH**

Attack
Vector

NETWORK

Attack
Complexity

LOW

Privileges
Required

NONE

User
Interaction

REQUIRED

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH
CVSS2 Score: 9.3 - HIGH			
Access Vector	Access Complexity	Authentication	
NETWORK	MEDIUM	NONE	
Confidentiality Impact	Integrity Impact	Availability Impact	
COMPLETE	COMPLETE	COMPLETE	

CVE References		
Description	Tags	Link
Externally Controlled Reference to a Resource in Another Sphere in MSEdgeRedirect · Advisory · rcmaehl/MSEdgeRedirect · GitHub	github.com text/html	CONFIRM github.com/rcmaehl/MSEdgeRedirect/security/advisories/GHSA-95v4-748v-fmf9
Release 0.5.0.1 - Security Fixes · rcmaehl/MSEdgeRedirect · GitHub	github.com text/html	MISC github.com/rcmaehl/MSEdgeRedirect/releases/tag/0.5.0.1
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

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Msedgeredirect Project	Msedgeredirect	All	All	All	All
cpe:2.3:a:msedgeredirect_project:msedgeredirect:*****:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
@CVEreport	CVE-2021-43844 : MSEdgeRedirect is a tool to redirect news, search, widgets, weather, and more to a user's default... twitter.com/i/web/status/1...	2021-12-20 21:23:43
/r/netcve	CVE-2021-43844	2021-12-20 22:38:37

© [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](#)