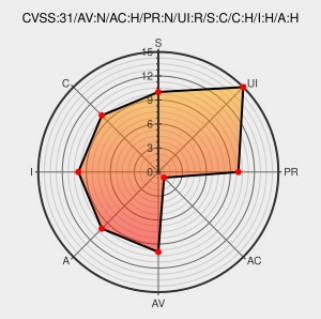
CVE-2022-23597

Published on: 02/01/2022 12:00:00 AM UTC

Last Modified on: 02/04/2022 05:20:00 PM UTC

CVE-2022-23597 - advisory for GHSA-mjrg-9f8r-h3m7

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Desktop from Element contain the following vulnerability:

Element Desktop is a Matrix client for desktop platforms with Element Web at its core. Element Desktop before 1.9.7 is vulnerable to a remote program execution bug with user interaction. The exploit is non-trivial and requires clicking on a malicious link, followed by another button click. To the best of our knowledge, the vulnerability has never been exploited in the wild. If you are using Element Desktop < 1.9.7, we recommend upgrading at your earliest convenience. If successfully exploited, the vulnerability allows an attacker to specify a file path of a binary on the victim's computer which then gets executed. Notably, the attacker does *not* have the ability to specify program arguments. However, in certain unspecified configurations, the attacker may be able to specify an URI instead of a file path which then gets handled using standard platform mechanisms. These may allow exploiting further vulnerabilities in those mechanisms, potentially leading to arbitrary code execution.

CVE-2022-23597 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 5.1 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality	**Integrity**	**Availability**

Impact	Impact	Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Remote program execution with user interaction · Advisory · vector-im/element-desktop · GitHub	github.com text/html	CONFIRM github.com/vector-im/element-desktop/security/advisories/GHSA-mjrg-9f8r-h3m7
Merge pull request from GHSA-mjrg-9f8r-h3m7 · vector-im/element-desktop@89b1e39 · GitHub	github.com text/html	MISC github.com/vector-im/element-desktop/commit/89b1e39b801655e595337708d4319ba4313feafa

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	Element	Desktop	All	All	All	All

cpe:2.3:a:element:desktop:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-23597 : Element Desktop is a Matrix client for desktop platforms with Element Web at its core. Element Des… twitter.com/i/web/status/1…	2022-02-01 11:52:13
/r/netcve	CVE-2022-23597	2022-02-01 12:38:05
/r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution - PATCH: NOW	2023-01-18 15:23:08

← Previous ID

Next ID→