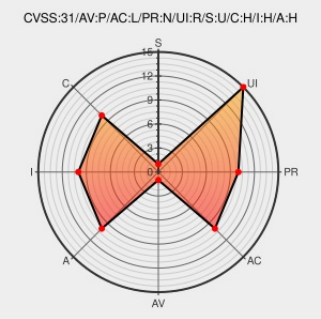
# CVE-2023-30024

Published on: Not Yet Published

Last Modified on: 05/12/2023 12:15:00 PM UTC

## CVE-2023-30024

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




Certain versions of A921 from Magicjack contain the following vulnerability:

The MagicJack device, a VoIP solution for internet phone calls, contains a hidden NAND flash memory partition allowing unauthorized read/write access. Attackers can exploit this by replacing the original software with a malicious version, leading to ransomware deployment on the host computer. Affected devices have firmware versions prior to magicJack A921 USB Phone Jack Rev 3.0 V1.4.

CVE-2023-30024 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 6.6 - MEDIUM

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

### CVE References

| Description | Tags | Link |
|---|---|---|
| Update your browser to use Google Drive, Docs, Sheets, Sites, Slides, and Forms - Google Drive Help | drive.google.com<br>text/html | MISC drive.google.com/drive/folders/1cKd8hksThK610GPtBQ3du8DEkwKywIAi?usp=sharing |
| VoIP Phone Service \| Internet Home Phone Service Provider \| magicJack | www.magicjack.com<br>text/html | MISC www.magicjack.com/ |
| Red Teaming: 0x01 Click RCE via VoIP USB - Samurai security | samuraisecurity.co.uk<br>text/html | MISC samuraisecurity.co.uk/red-teaming-0x01-click-rce-via-voip-usb/ |
| | pastebin.com<br>text/plain | MISC pastebin.com/raw/irWcawp8 |

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 |
|---|---|---|---|---|---|---|
| Hardware | Magicjack | A921 | 3.0 | All | All | All |
| Operating System | Magicjack | A921 Firmware | 1.4 | All | All | All |

cpe:2.3:h:magicjack:a921:3.0:*:*:*:*:*:*:*

cpe:2.3:o:magicjack:a921_firmware:1.4:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @CVEreport | CVE-2023-30024 : Insecure Permissions vulnerability found in MagicJack A921 USB Phone Jack Rev 3.0 v.1.4 allows a p… twitter.com/i/web/status/1… | 2023-04-28 13:11:07 |

← Previous ID

Next ID→