



CVE-2022-29472

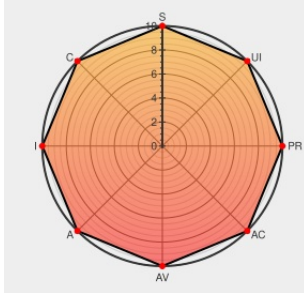
Published on: Not Yet Published

Last Modified on: 10/26/2022 03:22:00 PM UTC

CVE-2022-29472

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

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H



Certain versions of [Iota All-in-one Security Kit](#) from [Goabode](#) contain the following vulnerability:

An OS command injection vulnerability exists in the web interface `util_set_serial_mac` functionality of Abode Systems, Inc. [iota All-In-One Security Kit 6.9X](#) and [6.9Z](#). A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can send an HTTP request to trigger this vulnerability.

CVE-2022-29472 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [cisco](#) **abode systems, inc. - iota All-In-One Security Kit version = 6.9X**

Affected Vendor/Software: [cisco](#) **abode systems, inc. - iota All-In-One Security Kit version = 6.9Z**

CVSS3 Score: **9.8 - CRITICAL**

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

CVE References

Description	Tags	Link
TALOS-2022-1566 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2022-1566

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

Exploit/POC from Github

An OS command injection vulnerability exists in the web interface util_set_serial_mac functionality of Abode Systems,...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Goabode	Iota All-in-one Security Kit	-	All	All	All
Operating System	Goabode	Iota All-in-one Security Kit Firmware	6.9x	All	All	All
Operating System	Goabode	Iota All-in-one Security Kit Firmware	6.9z	All	All	All
cpe:2.3:h:goabode:iota_all-in-one_security_kit:-:*:*:*:*:*:*:						
cpe:2.3:o:goabode:iota_all-in-one_security_kit_firmware:6.9x:*:*:*:*:*:*:						
cpe:2.3:o:goabode:iota_all-in-one_security_kit_firmware:6.9z:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-29472 : An OS command injection vulnerability exists in the web interface util_set_serial_mac functionalit... twitter.com/i/web/status/1...	2022-10-25 17:18:47
 /r/netcve	CVE-2022-29472	2022-10-25 18:38:47

[← 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](#)