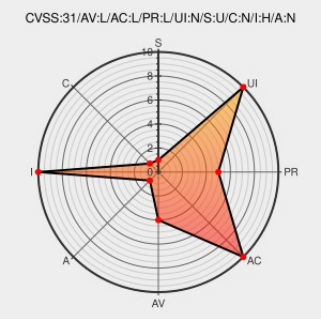
CVE-2023-32076

Published on: Not Yet Published

Last Modified on: 05/18/2023 09:22:00 PM UTC

CVE-2023-32076 - advisory for GHSA-wc64-c5rv-32pf

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



Certain versions of In-toto from In-toto Project contain the following vulnerability:

in-toto is a framework to protect supply chain integrity. The in-toto configuration is read from various directories and allows users to configure the behavior of the framework. The files are from directories following the XDG base directory specification. In versions 1.4.0 and prior, among the files read is `.in_totorc` which is a hidden file in the directory in which in-toto is run. If an attacker controls the inputs to a supply chain step, they can mask their activities by also passing in an `.in_totorc` file that includes the necessary exclude patterns and settings. RC files are widely used in other systems and security issues have been discovered in their implementations as well. Maintainers found in their conversations with in-toto adopters that `in_totorc` is not their preferred way to configure in-toto. As none of the options supported in `in_totorc` is unique, and can be set elsewhere using API parameters or CLI arguments, the maintainers decided to drop support for `in_totorc`. in-toto's `user_settings` module has been dropped altogether in commit 3a21d84f40811b7d191fa7bd17265c1f99599afd. Users may also sandbox functionary code as a security measure.

CVE-2023-32076 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **in-toto** - **in-toto** version **= <= 1.4.0**

CVSS3 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
Merge pull request from GHSA-wc64-c5rv-32pf · in-toto/in-toto@3a21d84 · GitHub	github.com text/html	MISC github.com/in-toto/in-toto/commit/3a21d84f40811b7d191fa7bd17265c1f99599afd
XDG Base Directory Specification	specifications.freedesktop.org text/html	MISC specifications.freedesktop.org/basedir-spec/basedir-spec-latest.html
Configuration Read From Local Directory · Advisory · in-toto/in-toto · GitHub	github.com text/html	MISC github.com/in-toto/in-toto/security/advisories/GHSA-wc64-c5rv-32pf
Functionaries Do Not Perform Verification · Advisory · in-toto/docs · GitHub	github.com text/html	MISC github.com/in-toto/docs/security/advisories/GHSA-p86f-xmg6-9q4x

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	In-toto Project	In-toto	All	All	All	All

cpe:2.3:a:in-toto_project:in-toto:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-32076 : in-toto is a framework to protect supply chain integrity. The in-toto configuration is read from v… twitter.com/i/web/status/1…	2023-05-10 18:08:31

← Previous ID

Next ID→