

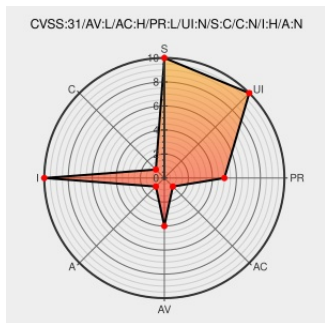


CVE-2021-41087

Published on: 09/21/2021 12:00:00 AM UTC

Last Modified on: 10/05/2021 04:30:00 PM UTC

CVE-2021-41087 - advisory for GHSA-vrxp-mg9f-hwf3

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

Certain versions of [in-toto-golang](#) from [in-toto](#) contain the following vulnerability:

in-toto-golang is a go implementation of the in-toto framework to protect software supply chain integrity. In affected versions authenticated attackers posing as functionaries (i.e., within a trusted set of users for a layout) are able to create attestations that may bypass DISALLOW rules in the same layout. An attacker with access to trusted private keys, may issue an attestation that contains a disallowed artifact by including path traversal semantics (e.g., foo vs dir/../foo). Exploiting this vulnerability is dependent on the specific policy applied. The problem has been fixed in version 0.3.0.

CVE-2021-41087 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [in-toto](#) - [in-toto-golang](#) version < 0.3.0

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description

Tags

Link

Merge pull request from GHSA-vrxp-mg9f-hwf3 · in-toto/in-toto-golang@f2c57d1 · GitHub

github.com

text/html

MISC

github.com/in-toto/in-toto-golang/commit/f2c57d1e0f15e3ffbeac531829c696b72ecc4290

Improperly Implemented path matching for in-toto-golang · Advisory · in-toto/in-toto-golang · GitHub

github.com

text/html

CONFIRM

github.com/in-toto/in-toto-golang/security/advisories/GHSA-vrxp-mg9f-hwf3

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.

Related QID Numbers

980518 Go (go) Security Update for github.com/in-toto/in-toto-golang (GHSA-vrxp-mg9f-hwf3)

Known Affected Configurations (CPE V2.3)

Type

Vendor

Product

Version

Update

Edition

Language

Application

In-toto

In-toto-golang

All

All

All

All

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

No vendor comments have been submitted for this CVE

Social Mentions

Source

Title

Posted (UTC)

@CVEreport

CVE-2021-41087 : in-toto-golang is a go implementation of the in-toto framework to protect software supply chain in... twitter.com/i/web/status/1...

2021-09-21 21:10:52

@torresariass

Whoa, in-toto-golang (and the whole in-toto ecosystem) got its first CVE: CVE-2021-41087 cve.circl.lu/cve/CVE-2021-41087... twitter.com/i/web/status/1...

2021-09-21 22:38:28

@ipssignatures

I know no IPS that has a protection/signature/rule for the vulnerability CVE-2021-41087. The vuln was published 0 d... twitter.com/i/web/status/1...

2021-09-22 02:04:01

@ipssignatures

The vuln CVE-2021-41087 has a tweet created 0 days ago and retweeted 8 times. [twitter.com/torresariass/s... #Sgah5y4qwsqqe2](https://twitter.com/torresariass/status/1484549444444444444)

2021-09-22 02:04:01

@ipssignatures

The vuln CVE-2021-41087 has a tweet created 0 days ago and retweeted 11 times. [twitter.com/torresariass/s... #pow1rtrtwwcve](https://twitter.com/torresariass/status/1484549444444444444)

2021-09-22 06:06:00

@threatmeter

CVE-2021-41087 in-toto-golang is a go implementation of the in-toto framework to protect software supply chain inte... twitter.com/i/web/status/1...

2021-09-22 07:09:52

← Previous ID

Next ID →

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](#)